



Stratus® Continuous Processing® Technology

Automatic 99.999% Uptime for
Microsoft® Windows® Server® Environments



Abstract

Server virtualization and cloud computing bring new benefits and capabilities to IT organizations, but not without their own set of challenges and risks. As x86 virtualization has become established and cloud computing emerges, a robust IT infrastructure actually matters more than ever. Software aspects get most of the attention partly because they are new. Despite the hype, not every technical challenge is better solved by software alone because of the tradeoffs involved. For high-performance, high-density or mission-critical services and applications, using fault-tolerant server hardware hardens against new vulnerabilities and complements the resilience you can achieve with Microsoft Hyper-V virtualization and cloud computing.

Stratus Technologies' family of fault-tolerant ftServer[®] systems is proven to deliver industry-leading uptime of 99.999% and greater for Microsoft[®] Windows[®] and Microsoft[®] Hyper-V[™] environments. The source of this immediate, transparent availability protection is the Stratus[®] Continuous Processing[®] technology built into every ftServer system, which enables *The Smarter Approach to Uptime*[™].

Virtually any software application designed for the Windows operating environment will run **unchanged and unmodified** on servers that are specifically designed to prevent unplanned downtime.

By engineering robustness directly into the server's hardware, software, and serviceability, Stratus offers customers a line of industry-standard, Intel[®] processor-based servers that deliver unsurpassed availability while providing operational simplicity and a significant financial advantage over competing high-availability clusters.

This paper presents an overview of Stratus Continuous Processing technology as implemented in the fifth generation of the ftServer family. Fundamentals behind the Continuous Processing design — lockstep technology, failsafe software, and the ActiveService[™] architecture — are explained in detail.

Contents

<i>Automatic 99.999% Uptime for Microsoft® Windows® Server® Environments</i>	1
Fundamentals of Continuous Processing Design	4
Lockstep Technology	6
Dual Modular Redundancy (DMR)	7
Industry-Standard, Modular Components	7
Failsafe Software	7
Transient Hardware Errors	8
Hardened Device Drivers	8
Open-Driver Technology.....	9
Software Issues Analyzed and Corrected	9
<i>Automatic Reboot</i>	10
<i>Failsafe System Software</i>	10
In-Memory Data Maintained.....	11
<i>Quick Dump</i>	11
<i>Rapid Disk Resynchronization (RDR)</i>	11
Extensive Testing	12
ActiveService Architecture	12
Built-in Serviceability	12
Reduced Exposure to Operator Error	13
Virtual Technician Module.....	14
ActiveService Network	14
ftGateway™ Software.....	14
ActiveService Manager	15
Stratus ftService SM Options	15
Focus on Mission-Critical Services.....	15
Conclusion	16
Additional Resources	17
Abbreviations and Acronyms	17

Fundamentals of Continuous Processing Design

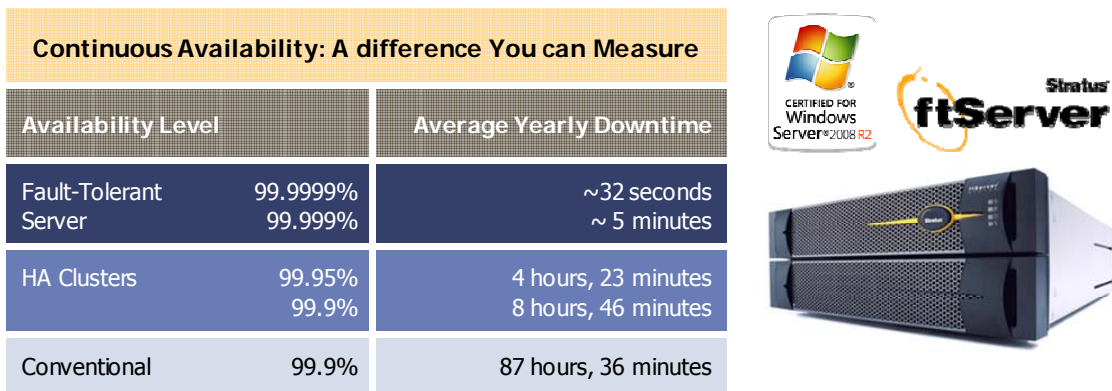
To provide the most complete protection for uptime possible, a comprehensive server solution must address the areas of hardware, software, and service. Only Stratus Technologies, together with its distribution channel partners, and ftServer systems provide this total solution in the Windows market.

Every Stratus ftServer system includes Continuous Processing features that are the outgrowth of more than a quarter century's experience of ensuring uptime for demanding mission-critical and business-critical applications around the world.

All aspects of the Continuous Processing design work concurrently to prevent unplanned downtime, not simply minimize it. 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 when one of the servers in the cluster fails). Stratus describes this unequaled availability and reliability protection as *The Smarter Approach to Uptime*. Unlike reliability-enhancing approaches that are not integral to a server’s design, built-in continuous availability helps limit exposure to the operator error that industry experts identify as a leading cause of unplanned downtime.

Notably, off-the-shelf Windows-based applications need not be modified in any way to benefit from these exceptional availability safeguards. This advantage represents a considerable improvement compared with clusters that require failover scripting, repeated test procedures, and software changes to make applications cluster-aware.

Figure 1: Automatic >99.999% Uptime for Windows Environments



Windows applications automatically from Stratus availability safeguards – without ANY modifications

Figure 2: Core Elements of the Stratus Continuous Processing Design



Stratus enables Continuous Processing capabilities in ftServer systems through three fundamental elements:

- **Lockstep Technology** — Lockstep technology uses 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. The system also detects and corrects transient hardware errors that could cause software failures if left unchecked.

Beginning with the second-generation ftServer family and continuing with the third-generation additions, Stratus has advanced its lockstep hardware design with distinct improvements. Enhancements to the servers' physical design and the increased use of industry-standard, modular components provide superior price-performance, greater space efficiency, better investment protection, and simpler serviceability. (The *Lockstep Technology* and *ActiveService Architecture* sections of this paper supply more information about these advantages.)

- **Failsafe Software** — Failsafe software works in concert with lockstep technology to prevent many software errors from escalating into outages. Unlike typical servers or clusters, ftServer hardware and software handles 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.

Management and diagnostic features capture, analyze, and notify Stratus of any software issues. This allows support personnel to take a proactive approach to correcting software problems before they recur. In addition, hardened device drivers add considerable reliability to the Windows environment on Stratus ftServer systems.

- **ActiveService Architecture** — An unmatched combination of ActiveService capabilities enables built-in serviceability not offered by other vendors. Stratus ftServer systems constantly monitor their own operation. When a fault is detected, the server correctly isolates the condition and automatically opens a call that tells the Stratus support center exactly what action to take.

Remote support capabilities, which are made possible by the system's new Virtual Technician Module and the global ActiveService Network, enable Stratus service engineers

to troubleshoot and resolve problems online more than 95% of the time. If necessary, the system automatically orders its own hot-swappable replacement part and ensures the correct part is delivered, within 24 hours, to major locations worldwide. Users can install these components easily while the ftServer system continues to run uninterrupted. In addition, a secure Web-based ActiveService Manager allows Stratus and customer-authorized vendors to collaborate on faster problem resolution.

The following pages provide a closer look at each of these three aspects of Continuous Processing technology.

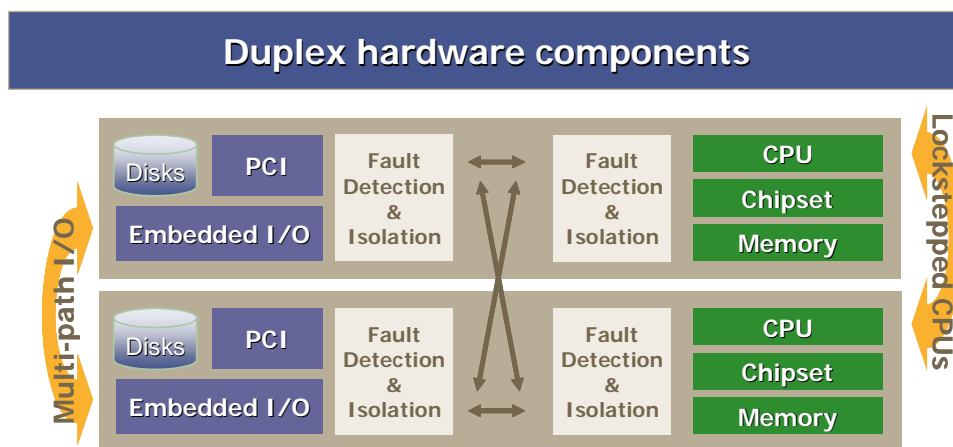
Lockstep Technology

The ftServer family eliminates single points of failure using replicated components that continue uninterrupted processing — even in the event of a component malfunction. Hardware faults are handled automatically by the system, without failover delay or data loss.

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.

While many servers offer duplicated power supplies, fans, and disk drives, only Stratus provides protection for core system components that include motherboards, processors, memory, I/O buses, and I/O adapters. Another advantage of this approach is that an ftServer system presents a single-system view and runs a single copy of all software, which typically reduces software licensing costs and simplifies administration as compared with multi-node cluster alternatives.

Figure 3: ftServer Lockstep Technology



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: SCSI, SAS, Ethernet, remote management, and Fibre Channel. Internal SAS disk storage, along with expansion ftScalable 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.

Dual Modular Redundancy (DMR)

Stratus offers ftServer systems in a standard dual modular redundancy (DMR) mode, which uses two CPU-memory assemblies (motherboards). These systems deliver levels of availability unrivaled by competitive cluster systems. DMR systems are designed for “five nines” (99.999%) of availability, and field experience to date shows performance that surpasses these design goals.

As previously described, all motherboards run in a lockstep manner from a single system clock source. 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 brings the benefits of Stratus’ traditional “pair-and-spare architecture” to a design that is simpler and requires fewer components. Leveraging off-the-shelf technology in a modular physical design not only captures a new cost advantage, but it also reduces development time and improves time to market for new ftServer models.

In fact, the ftServer product line takes full advantage of standard Intel server components and designs. The biggest differences from conventional servers are that the ftServer line separates PCI I/O from the rest of the motherboard and adds fault-detection hardware logic — Stratus’ custom chipsets — which are essential for lockstep operation and effective fault detection and isolation.

Failsafe Software

Stratus ftServer systems support the Microsoft Windows Server[®], Datacenter Edition, Enterprise Edition and Standard Edition operating systems as bare-metal or Hyper-V configurations, with additional software availability features provided by Stratus.

The ftServer family running Windows has demonstrated hardware, hypervisor, and operating system availability levels beyond 99.999%, as measured by actual production system data. Windows Server 2003 brought new reliability features to the proven Windows base, including hot-plug PCI, memory mirroring, load balancing and failover for miniport drivers, and multipath I/O. Windows Server 2008 further increased the reliability, security, and ease of use of the Windows Operating System. These Windows features help to enhance the impressive uptime performance of the ftServer series.

Stratus' addition of failsafe software capabilities addresses known sources of system and application failures, and minimizes downtime during repair or maintenance:

- Software is shielded from transient hardware errors.
- Hardened drivers prevent software failures.
- Embedded open-driver technology allows qualified third-party device drivers to access hardening capabilities.
- Software issues are reliably captured, analyzed, and corrected.
- In-memory data is maintained.
- Extensive integration and error-insertion testing finds and resolves difficult errors.

Since Microsoft implements Hyper-V as an integrated feature of the operating system, all of Stratus' failsafe software capabilities apply equally and seamlessly to both Hyper-V and bare-metal Windows installations.

All of these software enhancements are implemented without affecting the Windows core operating system code. As a result, systems maintain 100% application binary interface (ABI) compatibility with Windows Server operating systems. All ftServer systems pass the same rigorous Windows Hardware Compatibility Tests (HCT) as other servers, ensuring that virtually any Windows application runs without modification on Stratus ftServer systems. All current models are listed on the Microsoft Hardware Compatibility List (HCL).

Transient Hardware Errors

The ftServer hardware and system software is designed to detect, isolate, and automatically recover from transient errors as well as hard errors. Because error handling is a known vulnerability in software design, the masking of both transient and hard errors averts many potential software problems. The ftServer hardware and system software 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.

Hardened Device Drivers

Errant device drivers are acknowledged as a root cause for many Windows operating system crashes. For example, Microsoft estimated that device-driver errors caused more than 30% of all Windows NT[®] 4.0 reboots. With the Windows 2000 Server, Windows Server 2003, and Windows Server 2008 operating systems, Microsoft introduced significant improvements to driver reliability through new testing and certification programs. But with the advances in Windows 2000, 2003, and 2008 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 Windows 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 and a service interface conforming to Microsoft's Windows Management Instrumentation (WMI) driver model.

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 hot insertion and removal of adapters (also known as surprise insertion and surprise removal)
- Transparent failover (except for tape and asynchronous communication adapters)
- Ability to run online diagnostics
- Support for online firmware updates
- Monitoring and reporting through WMI

Open-Driver Technology

Starting with ftServer System Software release 3.0, most of the code changes required to harden device drivers has been separated from the device-specific driver and moved to a separate layer of code within the driver stack. With this embedded open-driver technology, vendor source code is no longer needed to produce a hardened driver. The vendor driver must, however, pass the Microsoft Windows WHQL tests including support for Plug-and-Play surprise removal. It is still recommended that drivers be fully tested, including testing with the Stratus fault-insertion test tools to ensure driver reliability.

Software Issues Analyzed and Corrected

Software-related problems can occur even with the best of preventive measures. The system design provides a considerable initial advantage in correcting these software issues by reliably distinguishing software problems from hardware problems. With conventional servers or high-availability clusters, many problems attributed to software are actually caused by transient hardware errors. Because systems automatically detect, isolate, and resolve transient hardware errors, issues are immediately separated into the appropriate category — greatly contributing to effective and timely problem resolution.

More important, the ftServer design 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.

The ftServer hardware and system software trap and handle transient hardware/software errors that a cluster node or conventional system would propagate to the operating system, middleware, or application software. Since improper error handling is known to cause many software problems, masking many normal errors decreases the likelihood of software problems on ftServer systems. Another advantage of the architecture is the ability of the hardware, software enhancements, and service features to assist in isolating and correcting Windows operating system and device driver failures.

Two major features mitigate software-related problems:

- Automatic reboot
- Failsafe system software

Automatic Reboot

In the unlikely event that an operating system crash occurs, Stratus ftServer systems automatically reboot while preserving crash information in one of the replicated CPU-memory units. A kernel memory dump is automatically taken after the system and application are back online. Cumbersome shipments of dump information are avoided because ftServer systems support remote crash analysis over the Stratus ActiveService Network.

The ftServer system's monitoring software identifies and reports many software problems, such as resource exhaustion or performance problems. This allows corrective action to occur before there is a negative impact on applications. Software also tracks system configuration and revision levels, helping to identify potential incompatibility issues and assisting in analysis of any problems that may occur.

Failsafe System Software

Stratus has developed failsafe system software to create an availability-supporting ecosystem for the ftServer family. This system software provides reliability and fault-tolerant features for I/O devices, performs monitoring and management of the server, enables remote service and support, and offers other advanced availability features.

Failsafe system software features include the following:

- **ftServer Active Upgrade™ technology** — This first-of-its-kind technology for fault-tolerant Microsoft Windows operating system environments enables customers to perform online software upgrades and critical operating system hot fixes without having to take the server or application offline for extended periods. Active Upgrade technology adds a new availability dimension beyond the field-proven 99.999% uptime protection for which Stratus servers are known.

Made possible by the next-generation Stratus-designed chipset in the ftServer third-generation systems, Active Upgrade technology enables online upgrading by splitting the fully redundant system into two independently running servers. While one server continues to run the application without interruption, software updates are applied to the other server. The two sides are then synchronized and returned to fault-tolerant operation as one logical server.

- **ftServer Management Console (ftSMC)** — This user interface allows an administrator to configure, control, and generate detailed status information for ftServer systems. The ftSMC is a snap-in added to the standard Microsoft Management Console (MMC). The ftSMC snap-in runs locally on any ftServer system, or remotely on any Windows system. Both local and remote ftServer systems can be managed from any instance of the ftSMC.
- **Simple Network Management Protocol (SNMP) Agent** — The ftServer SNMP Agent extends the Microsoft SNMP Agent, allowing third-party enterprise management consoles to remotely monitor ftServer systems. Most enterprise management software — including the Tivoli® Enterprise Console, HP® OpenView®, and CA Unicenter® products — supports SNMP.

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 MIB file is provided to allow the enterprise management software packages to understand Stratus alarms.

In-Memory Data Maintained

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. Stratus ftServer systems protect in-memory data from hardware failures using a lockstep architecture that stores memory contents in at least two separate hardware components.

Stratus ftServer systems provide key capabilities that preserve in-memory data:

- Quick dump
- Rapid disk resynchronization (RDR)

Quick Dump

With conventional Windows servers, users have to make an uncomfortable choice after a crash. Either they can keep the application down while they take a system memory dump to be analyzed later, or get the application back up right away — but they lose the information that would help prevent a similar crash in the future. With ftServer systems, users no longer face this dilemma; they can minimize the time applications are offline and capture diagnostic information.

The quick dump capability capitalizes on the replicated hardware in fault-tolerant ftServer systems. In the event of an operating system software failure, an ftServer system 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 CAC to report the problem. Through the new Virtual Technician Module — which is integral to Stratus' ActiveService Architecture — Stratus service professionals can immediately begin diagnosing the system dump and manage the problem to its resolution.

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.

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 from the mirrored 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.

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; errors are continuously simulated during the test process.

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 Windows 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.

ActiveService Architecture

As is true for other aspects of ftServer systems, the guiding design point of the ActiveService Architecture is the ability to detect and resolve problems *before* they cause system downtime. This architecture combines automatic fault detection, automatic fault isolation, integrated “call-home” remote support, and online component replacement to enable built-in serviceability that is unequalled by other servers.

The ActiveService architecture begins with the design of the hardware and its technology-enabled Access features and extends to Stratus’ global ActiveService Network and Web-based ActiveService Manager.

Figure 2: Active Service Architecture Highlights

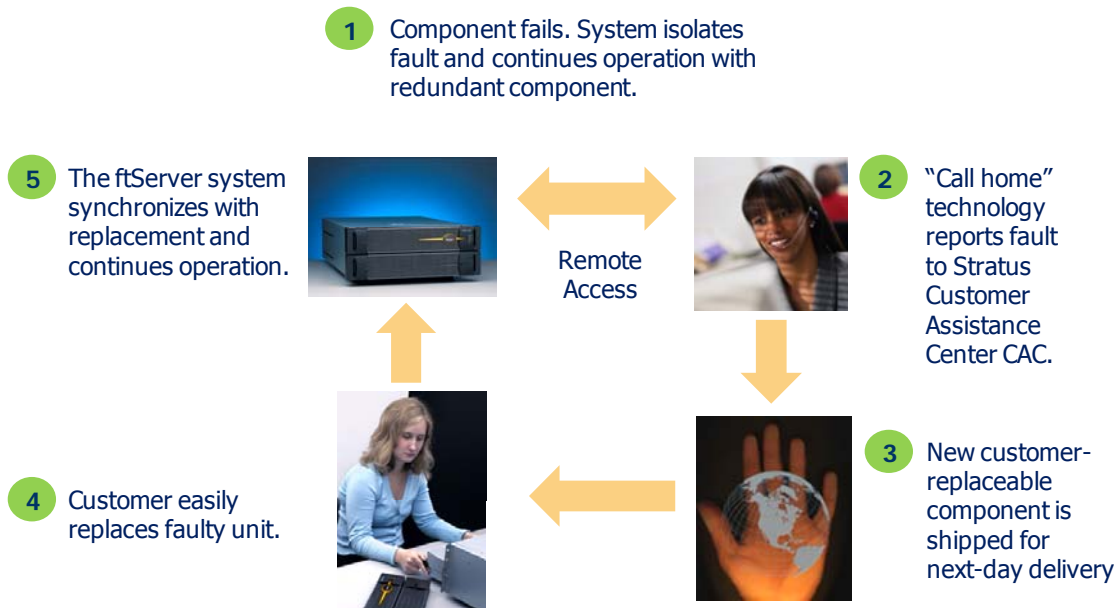


Built-in Serviceability

An example problem resolution scenario (*Figure 4*) demonstrates how the built-in serviceability features equip ftServer systems to protect uptime.

Simply stated, ftServer systems themselves include capabilities that provide the first level of customer support. Maintenance software within the server runs transparently to constantly monitor, diagnose, and report system events, accurately isolating faults to the component level. In the event of a hardware error or failure, the system automatically isolates the condition while continuing operation on a second, replicated component. In contrast with a cluster, there is no failover time and users do not experience a loss of performance.

Figure 3: Problem Resolution Scenario



The server automatically reports any problem condition to a Stratus Customer Assistance Center (CAC) via a secure, dialed connection. The global ActiveService Network (formerly known as the Stratus Service Network or SSN) provides a worldwide infrastructure that enables remote access to every customer system. Authorized support professionals are able to remotely investigate critical problems 24/7, without the need to visit the customer site. In practice, Stratus service engineers have been able to troubleshoot and resolve problems online in more than 95% of cases.

In service situations where a replacement component is needed, the ftServer system automatically orders the correct replacement part. Replacement parts ship for next-day delivery to most locations. Because most ftServer components are customer replaceable units (CRUs), the replacement part can be installed easily by a user, without requiring special tools or assistance from a field service engineer.

The ftServer system brings the newly installed component into operation automatically, synchronizing it in lockstep with its partner. The system and the application continue to run normally throughout the entire process.

Reduced Exposure to Operator Error

The preceding section illustrates the point that ftServer systems, from the very first models, are designed for online component replacement to simplify service and reduce exposure to operator error. The modular second- and third-generation ftServer families take this concept to the next level by reducing the number of system components and by tying components 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.

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 system that operates independently of the host computer.

The new Virtual Technician Module is Stratus' second-generation remote access technology. The Virtual Technician Module is implemented using a DIMM-style slot, so it frees up two PCI slots in the system. The Virtual Technician Module introduces new remote service capabilities including full remote keyboard, video and mouse, remote floppy/CD and out-of-band alerts.

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 on-site service.

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 capabilities, information capture and storage, and security features.

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.

ftGateway™ Software

The ftGateway software feature allows several ftServer systems to share a common dial-up connection to the Stratus ActiveService network. This capability limits the need for phone lines and makes it easier to manage service connections for multiple ftServer systems located at a single site.

One ftServer system (with a second acting as backup) provides a connection gateway for up to 20 systems. Only the gateway system need contain Virtual Technician Modules; other ftServer systems in the group connect to the gateway system via Ethernet using either Virtual technician Modules or standard Ethernet ports.

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.

Stratus ftServiceSM Options

Customers may choose from several levels of proactive ftServiceSM support options that make use of ActiveService technologies. The premier offering is Assured Availability PlusSM ftService coverage, which provides 24/7 support for ftServer systems and the Windows operating system.

This approach leverages the powerful ActiveService capabilities built into every ftServer system, connecting servers to a global service network for detecting, troubleshooting, and resolving problems fast — usually without the need for an on-site call. This is service with a difference: designed to prevent downtime instead of simply providing a remedy after the fact.

Third-party collaboration is also a standard part of Stratus ActiveService Network and Web support center. Stratus ftService customers may designate non-Stratus vendors to view the status of calls through the ActiveService Manager and the ActiveService Network, building a virtual call queue for collaborative problem solving from anywhere in the world.

Furthermore, Stratus is a Microsoft Gold Certified Partner for Enterprise Systems in the United States. Stratus' integrated electronic support infrastructure allows these premier Microsoft support services to be extended to customers worldwide.

Focus on Mission-Critical Services

Because large-scale deployments place greater demands upon IT departments, Stratus 24/7 Worldwide Services provides a range of professional services offerings that focus on achieving maximum uptime and performance for ftServer computing solutions. Services include design, implementation, and management of availability solutions, as well as training and education.

Stratus' start-of-the-art Center for Fault-Tolerant Computing, located at its U.S. headquarters in Maynard, Massachusetts, provides compliance and availability testing of third-party products and customer applications, in addition to benchmarking and porting services.

These options help customers implement reliable, cost-effective solutions without the extra overhead of bringing technical skills in-house, diverting their internal staff from other projects, or contracting with several firms to design and install the application and infrastructure.

Conclusion

While software-enabled virtualization and cloud computing allow IT services and applications to appear independent of the underlying resources, in several respects these computing models introduce stress points that demand *greater* robustness of the IT infrastructure. Using fault-tolerant server hardware for selected key roles within virtualized and cloud environments builds in reliability and reduces management complexity, helping to sustain the high service levels that enterprises can count on.

With the ftServer family, Stratus provides a practical and affordable way to achieve the highest levels of availability for Windows and Hyper-V environments. The ftServer line delivers Continuous Processing capabilities through lockstep technology, failsafe software, and the 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 unplanned downtime, not simply allow for quick recovery, as high-availability clusters and “robust” conventional servers are engineered to do. The fact that Continuous Processing features operate transparently and automatically means that no human intervention, or additional programming or testing, are required for Windows applications to benefit from a fully fault-tolerant server environment. Compared with reliability-enhancing approaches that are not intrinsic to a server’s design, enterprises can reduce their exposure to the operator error that industry experts cite as a leading cause of unplanned downtime.

The latest generation of systems expands these inherent 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 Continuous Processing capabilities offer a tangible financial advantage over competing approaches by reducing costs associated with complicated deployment, unplanned downtime, and ongoing support expenses.

Additional Resources

Stratus publishes a series of white papers that describe other technologies, features, and benefits offered by ftServer systems. These documents are available at <http://www.stratus.com/whitep/>

Abbreviations and Acronyms

ABI	application binary interface
CAC	(Stratus) Customer Assistance Center
CPU	central processing unit
CRU	customer replaceable unit
DMR	dual modular redundancy
ftSMC	ftServer Management Console
HCL	(Microsoft) Hardware Compatibility List
HCT	(Microsoft) Hardware Compatibility Tests
I/O	input/output
MIB	management information base
MMC	Microsoft Management Console
PCI	Peripheral Component Interconnect
RAID	Redundant Array of Independent Disks; originally Redundant Array of Inexpensive Disks
RDR	Rapid Disk Resynchronization
SCSI	Small Computer System Interface
SNMP	Simple Network Management Protocol
VTM	Virtual Technician Module
WMI	(Microsoft) Windows Management Instrumentation

Stratus, ftServer, the ftServer logo, and Continuous Processing are registered trademarks; The Smarter Approach to Uptime, ActiveService, Active Upgrade, ftGateway, the Stratus Technologies logo, and the Stratus 24x7 logo are trademarks; and ftService, Assured Availability, and Assured Availability Plus are service marks of Stratus Technologies Bermuda Ltd.

Microsoft, Hyper-V, Windows, Windows Server, and Windows NT are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Tivoli is a registered trademark of IBM Corporation. Intel is registered trademark of the Intel Corporation in the United States and other countries. HP and OpenView are registered trademarks of Hewlett-Packard Company. Unicenter is a registered trademark owned by Computer Associates International, Inc.

All other trademarks and registered trademarks are the property of their respective holders.

Specifications and descriptions are summary in nature and subject to change without notice.

© 2010 Stratus Technologies Bermuda Ltd. All rights reserved.
X935-D