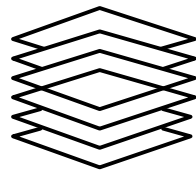


*PRIMEPOWER's System
Management Is the Key
to Its Quality of Service*

September 2002



*A D.H. Brown Associates, Inc. White Paper Prepared for
Fujitsu*

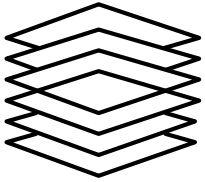
This document is copyrighted © by D.H. Brown Associates, Inc. (DHBA) and is protected by U.S. and international copyright laws and conventions. This document may not be copied, reproduced, stored in a retrieval system, transmitted in any form, posted on a public or private website or bulletin board, or sublicensed to a third party without the written consent of DHBA. No copyright may be obscured or removed from the paper. D.H. Brown Associates, Inc. and DHBA are trademarks of D.H. Brown Associates, Inc. All trademarks and registered marks of products and companies referred to in this paper are protected.

This document was developed on the basis of information and sources believed to be reliable. This document is to be used "as is." DHBA makes no guarantees or representations regarding, and shall have no liability for the accuracy of, data, subject matter, quality, or timeliness of the content. The data contained in this document are subject to change. DHBA accepts no responsibility to inform the reader of changes in the data. In addition, DHBA may change its view of the products, services, and companies described in this document.

DHBA accepts no responsibility for decisions made on the basis of information contained herein, nor from the reader's attempts to duplicate performance results or other outcomes. Nor can the paper be used to predict future values or performance levels. This document may not be used to create an endorsement for products and services discussed in the paper or for other products and services offered by the vendors discussed.

TABLE OF CONTENTS

MANAGEMENT OVERVIEW	1
RESOURCE MANAGEMENT	2
HIGH-AVAILABILITY MANAGEMENT.....	3
SECURITY MANAGEMENT.....	5
REVIEW OF KEY POINTS	5



PRIMEPOWER's System Management Is the Key to Its Quality of Service

Fujitsu's PRIMEPOWER servers offer IT departments the Solaris Operating Environment, Fujitsu's SPARC64 V microprocessor, and other technical advances designed for the highest levels of availability, flexibility, performance, scalability, and security. The optimum delivery of these PRIMEPOWER attributes requires the highest level of server system management capability.

This high level of system management offers IT departments assurance that all of the system's mission-critical attributes are available at the same time, all of the time. Managing the resources is critical. Otherwise, the quality of service falls and the attributes lose most, if not all, of their value to the information technology (IT) infrastructure user and the IT team responsible for providing and maintaining this infrastructure.

CIOs, CTOs, and other team members concerned with an organization's IT infrastructure should understand that Fujitsu provides all of PRIMEPOWER's mission-critical capabilities. To accomplish this, Fujitsu provides PRIMEPOWER system software and dedicated hardware facilities to manage the three key components of the server family's operation. These components include,

- computing resource management;
- high availability management; and
- security management.

It is not necessary that the CIO or CTO understand the details of these three capabilities. It is however, necessary that the overall functions be understood and that their benefits are clear. This white paper provides this overview. It is one in a series of seven PRIMEPOWER white papers that provide overviews of the complete PRIMEPOWER offering, PRIMECLUSTER, the Solaris Operating Environment, ARMTech software resource management, the PRIMEPOWER system architecture and the PRIMEPOWER SPARC64 V microprocessor.

MANAGEMENT OVERVIEW

Computing resource management covers the ability to use three PRIMEPOWER resource management capabilities. These capabilities include,

- Extended Partitioning (XPAR) and dynamic reconfiguration;
- resource allocation and sharing (ARMTech ShareEnterprise); and
- performance monitoring.

High-availability management spans the ability to use five PRIMEPOWER high-availability management capabilities. These capabilities include,

- autonomic monitoring and dynamic degradation;

- redundant configuration and IOMP (I/O Multipathing) software;
- failure analysis, reporting, and remote services;
- Solaris live upgrade and remote firmware update; and
- patch management.

Security management takes in the ability to use three PRIMEPOWER security management capabilities. These capabilities include,

- XPAR;
- firewalls and similar devices; and
- third-party offerings.

PRIMEPOWER's GUI-based WebSysAdmin browser accommodates the capability for XPAR in an integrated manner (see *Sidebar 1: Inside WebSysAdmin*).

RESOURCE MANAGEMENT

The ability to divide a single physical system into multiple virtual systems has long been available in mainframes. Today, such hardware partitioning is available for UNIX-based shared memory processing (SMP) machines.

Sidebar 1: Inside WebSysAdmin

WebSysAdmin is a GUI-based system management facility capable of handling multiple PRIMEPOWER systems. Using SNMP-based agents, WebSysAdmin allows connections to Computer Associates' Unicenter, IBM's Tivoli, and Fujitsu's SystemWalker enterprise system management frameworks and applications. Working on Windows or Solaris, WebSysAdmin allows the display of:

- ⇒ hierarchical domains and management of nodes and their interfaces;
- ⇒ hardware status (e.g., processors, memory) and configuration allocation;
- ⇒ system processes (with associated logs for individual or all domains);
- ⇒ user status (e.g., user definitions, group definitions, and passwords);
- ⇒ software management (e.g., packages and versions);
- ⇒ task management (e.g., task definition);
- ⇒ SNMP management (e.g., monitors and controls data passed to Unicenter or Tivoli); and
- ⇒ performance status (e.g., display of attributes of system performance).

PRIMEPOWER's hardware partitioning allows virtual system performance and quality of service. It also provides defective device isolation until repair can be accomplished and does so without taking the partition out of service. PRIMEPOWER also provides inter-partition security so that one virtual system is not a security risk to another. Each partition has a separate IP address. Such hardware partitioning is often of greater value than firmware-controlled software or logical partitioning wherein faults can affect other partitions that have joint resource ownership.

The newly introduced PRIMEPOWER XPAR makes it possible to achieve partition granularity down to one CPU and one GB of memory¹ (a part of a system board). This granularity is similar to that achieved traditionally with software partitioning, but the advantages of hardware partitioning are maintained.

¹ XPAR can achieve single processor partitions on the PRIMEPOWER 900 and 1500 models. The minimum PRIMEPOWER 2500 XPAR configuration contains two processors. For a fuller explanation, please refer to the companion white paper *PRIMEPOWER Server Architecture Excels in Scalability and Flexibility*.

Beyond this, PRIMEPOWER new series XPARs use dynamic reconfiguration to add or remove partition resources without taking the partition down. The partition continues to be highly available for user service. This flexibility is also similar to expectations derived from software partitioning.

In some instances, even the flexible XPARs are not sufficient to meet resource allocation needs. To address this, PRIMEPOWER offers ARMTech ShareEnterprise resource management software for CPUs in an XPAR (but not across XPARs). ARMTech Shares are designed to allocate resources where there is competition. Each party requesting resources is entitled to a portion of the sum of the shares held by all contesting resource consumers. By contrast, ARMTech Reservations provide a minimum resource guarantee in the event of a resource conflict. In other words, a reservation is an absolute percentage of a resource and cannot be overridden by a special request. (It is not demand-dynamic.)

Resource management is only possible if the status of the available PRIMEPOWER resources is known. PRIMEPOWER system administrators use monitoring tools to track the state of their partition or server resources. With the aid of such monitoring, administrators can review workloads and system performance, use dynamic reconfiguration to adjust resources to meet changing needs, and more.

HIGH-AVAILABILITY MANAGEMENT

To ensure the utmost in high availability, PRIMEPOWER monitors itself during system boot-up and system operation so that defective subsystems and components can be isolated. This keeps any effect on system availability to a minimum. In the long term, PRIMEPOWER's goal is to perform such detection and isolation autonomically without the need for human intervention.

PRIMEPOWER's System Control Facility (SCF) monitors PRIMEPOWER's processors, memory subsystem, operating system, and disk storage. SCF depends on an independent processor for its system management capabilities. It operates independently of the system's SPARC64 V microprocessors.

To do its job, the SCF processor and related software provide:

- supervisor functions to monitor possible problems with fans, CPUs, system temperature, and more;
- hot-swap support for the system board, power supply units, fans, and more in conjunction with system management software;
- hardware error logging to simplify fault location;
- partition management in conjunction with the system console; and
- I/O device supervision.

During system bootup, the SCF searches out the possibility of system "hangs" generated by hardware failures. If SCF identifies a defective, or potentially

defective device the system is restarted after the defect is isolated. The procedures involved, including whether or not a partially failed device is still used and when it should be replaced, are subject to the IT environment's operating policy. (Dynamic degradation is under the control of the system administrator.)

Even after the PRIMEPOWER has booted successfully, the SCF is monitored to detect undesired loop operation. Here too a failing or failed device is isolated to minimize the need to bring the system down. Should SCF be unable to isolate a loop-causing device dynamically (dynamic degradation) while the system is in operation, the device will be isolated during the necessary reboot. PRIMEPOWER's dynamic reconfiguration capability is used to replace devices isolated by dynamic degradation.

Sidebar 2: Inside REMCS

Fujitsu's Remote Customer Support System (REMCS) provides IT infrastructures using PRIMEPOWER with rapid, WAN-based, cost-effective remote aid for PRIMEPOWER installation, monitoring, maintenance, and management. REMCS allows,

- ⇒ monitoring, diagnostics, and setup of PRIMEPOWER configurations;
- ⇒ expert investigation of firmware, middleware, operating system, and application issues;
- ⇒ automated latest firmware and patch installation;
- ⇒ avoidance of resource constraint problems through monitoring the status and utilization trends of CPU, memory, and disk; and
- ⇒ rapid problem resolution through accesses to the PRIMEPOWER IT environment.

In short, REMCS manages the PRIMEPOWER IT resource. It accomplishes this task through the use of REMCS agents on PRIMEPOWER and a REMCS management server at the customer site that reports to the remote REMCS control center. All of this is configured based on the support policies of the environment using PRIMEPOWER.

The PRIMEPOWER new series takes the high-availability management capabilities discussed above even further. For example, it is now possible to minimize system downtime when a defective system board is replaced. The flexible memory architecture (FMA) feature supports such hot swapping even if the system board is loaded with the Solaris kernel (a kernel-loaded system board could not be hot swapped with previous PRIMEPOWER servers).

High-availability advantages do not stop here. The combination of redundant hardware interfaces for disk and network subsystems, working in cooperation with I/O Multipathing (IOMP) support software, allows the reconfiguration of new series I/O in the event of a failure. I/O possesses other flexibility designed to ensure high availability. For example, PCI Hot Plug (PHP) allows network paths to be dynamically changed while also allowing the dynamic swapping or adding of external I/O subsystems.

Keeping the system updated to the latest software version of firmware, patches, and operating system to ensure high-availability management is a topic of keen interest to IT executives. Wherever possible, consistent with IT policies in place, such software should be kept up-to-date to ensure the most flexible, bug-free system operation.

Those high-end installations connected to the Fujitsu Remote Customer Support System (REMCS) can enjoy the secure and automatic downloading of the latest firmware and patches (see *Sidebar 2: Inside REMCS*). Installations that need to change their Solaris version will likewise enjoy Solaris' ability to perform rolling operating system upgrades. They can also go back to the original operating system version if there is an issue that prevents a successful upgrade.

SECURITY MANAGEMENT

PRIMEPOWER's XPAR, as explained earlier, offers the advantages of hard partitioning together with the granularity capabilities of software partitions. The hard boundaries between XPARs prevent users and applications in one XPAR from any security violations of another XPAR.

Recognizing that an enterprise environment, to be fully secure, requires far more, Fujitsu provides PRIMEPOWER and third-party-based security management capabilities. These include,

- Security for the System Management Console (SMC) required for the PRIMEPOWER new series 900/1500/2500. The SMC acts as its own firewall and ensures that connections to the REMCS are encrypted. The REMCS itself has a variety of security features such as firewalls, registration and authentication, and encryption. WebSysAdmin on the SMC uses the TCP/IP Secure Sockets Layer (SSL) protocol and its own administrative LAN (if desired) for security between WebSysAdmin clients, servers, and agents.
- Solaris Operating Environment security, which includes an integrated firewall and IPSec security functions for data integrity and protection. IPSec ensures that IP snooping and spoofing cannot succeed and IPSec SSL-based encryption allows VPNs even over the public Internet. Solaris also uses the MIT Kerberos user authentication system.
- Third-party package support for a variety of scalable firewalls, trusted operating systems, VPNs, intrusion detection, enterprise security management packages, real-time monitoring, and more.

Combinations of these security offerings, based on an IT environment's security policies, provide PRIMEPOWER installations with the highest achievable security levels.

REVIEW OF KEY POINTS

This white paper has briefly described – from the viewpoint of an IT executive – PRIMEPOWER's capabilities for computing resource management, high-availability management, and security management. Clearly, PRIMEPOWER provides both state-of-the-art and industry-standard system management capabilities for computing resource management, high-availability management, and security management. These features are the basis for PRIMEPOWER's ability to deliver a high quality of service to the IT environment. Some of these capabilities are available in current PRIMEPOWER servers. Other capabilities are unique to the newly introduced PRIMEPOWER new series.

PRIMEPOWER's system management capabilities are industry leading. When these system management capabilities are combined with PRIMEPOWER's performance, scalability, cost-of-ownership, high availability, industry-leading microprocessor and server architecture along with the industry-standard Solaris

Operating Environment, PRIMEPOWER stands as a short-list candidate for single SMP server or clustered SMP server operation. Further information concerning these PRIMEPOWER attributes can be found in the other six white papers in this series, and on the Fujitsu websites.