Single-system reliability, availability, and serviceability on HP Integrity Superdome with emphasis on HP-UX

### Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction and executive summary</td>
<td>3</td>
</tr>
<tr>
<td>RAS philosophy</td>
<td>3</td>
</tr>
<tr>
<td>High availability on Madison-based HP Integrity Superdome systems</td>
<td>4</td>
</tr>
<tr>
<td>Fault management and fault tolerance</td>
<td>4</td>
</tr>
<tr>
<td>System-level reliability and availability</td>
<td>4</td>
</tr>
<tr>
<td>Memory—dynamic memory resiliency</td>
<td>6</td>
</tr>
<tr>
<td>Address/control parity protection</td>
<td>8</td>
</tr>
<tr>
<td>CPU—dynamic processor resiliency</td>
<td>8</td>
</tr>
<tr>
<td>I/O</td>
<td>8</td>
</tr>
<tr>
<td>Dual-patched I/O</td>
<td>8</td>
</tr>
<tr>
<td>I/O card isolation</td>
<td>8</td>
</tr>
<tr>
<td>I/O card qualification</td>
<td>9</td>
</tr>
<tr>
<td>PCI card OLA/OLR</td>
<td>9</td>
</tr>
<tr>
<td>Fabric (system crossbar) backplane</td>
<td>9</td>
</tr>
<tr>
<td>Cabinet infrastructure</td>
<td>9</td>
</tr>
<tr>
<td>Power infrastructure</td>
<td>9</td>
</tr>
<tr>
<td>Cooling infrastructure</td>
<td>10</td>
</tr>
<tr>
<td>Management processor (MP)</td>
<td>10</td>
</tr>
<tr>
<td>Other dynamic hardware features</td>
<td>10</td>
</tr>
<tr>
<td>Instant Capacity on Demand (iCOD) through HP-UX</td>
<td>10</td>
</tr>
<tr>
<td>Expected HP Integrity Superdome availability</td>
<td>11</td>
</tr>
<tr>
<td>HP-UX reliability and availability features</td>
<td>11</td>
</tr>
<tr>
<td>Serviceability and fault management</td>
<td>13</td>
</tr>
<tr>
<td>Fault management</td>
<td>13</td>
</tr>
<tr>
<td>Lower risk of downtime due to faults</td>
<td>14</td>
</tr>
<tr>
<td>Minimized downtime required to recover from faults</td>
<td>14</td>
</tr>
<tr>
<td>Problem resolution is easy and low cost; lower TCO</td>
<td>14</td>
</tr>
<tr>
<td>Improved total customer experience</td>
<td>15</td>
</tr>
<tr>
<td>Serviceability</td>
<td>15</td>
</tr>
</tbody>
</table>
Introduction and executive summary

HP Integrity Superdome runs the new 1.5 GHz Intel® Itanium® 2 (Madison) processors. It also uses an entirely new generation chipset called the sx1000 chipset. The sx1000 provides twice the memory bandwidth and 1.6 times the CPU bandwidth compared to the previous Superdome chipset. However, the major innovation for HP Integrity Superdome is the ability to run multiple operating systems simultaneously in different hard partitions. HP-UX, Windows® Server 2003, and Linux are planned to run on HP Integrity Superdome, and an investigation is underway to add OpenVMS to this list.

Existing Superdomes can be field upgraded to HP Integrity Superdome by removing the PA-RISC cell boards, replacing them with HP Integrity Superdome Madison cell boards, and upgrading required system firmware.

The objective of this white paper is to clearly present the reliability, availability, and serviceability (RAS) features of HP Integrity Superdome, and the underlying philosophy of RAS on HP Integrity Superdome. RAS was one of the highest-priority design objectives of HP Integrity Superdome. This paper will also highlight the RAS features of HP-UX, referring to how these features are supported or differ on Windows and Linux. Another objective of this paper is to educate and make clear the RAS characteristics so they can be compared with the competitors’ features. The final objective is to communicate the emphasis and importance HP puts on RAS in this mission-critical, high-end server.

This paper covers all of the major RAS features of HP Integrity Superdome. It is limited to HP Integrity Superdome and does not cover midrange or NonStop servers. This paper is also limited to the RAS capabilities of the single-system HP Integrity Superdome. HP has a full range of multi-system high-availability solutions that are described in the white paper available from HP titled High availability and business continuity solutions for HP Integrity servers.

The major competitors to HP Integrity Superdome are the IBM p690 and the Sun 15000 in the RISC processor space and the Unisys ES7000 in the Itanium processor space.

RAS philosophy

The RAS philosophy is an industry approach to describing the reliability, availability, and serviceability of a computer system. HP ties RAS features to its higher-level value propositions: high availability (HA) and total cost of ownership (TCO).

Figure 1. Customer modeling for RAS

HP uses the RAS model to explain the relationship of reliability, availability, and serviceability to our key market drivers of high availability (HA) and total cost of ownership (TCO).
High availability on Madison-based HP Integrity Superdome systems

The purpose of the HP Integrity Superdome RAS feature set is to address the real causes of customer downtime and costs due to downtime. These causes and costs are determined by actual field data from high-end computer users. The real goal of HA and TCO is to maximize the application availability seen by the end customer and to minimize the cost of owning a computer system.

Figure 2. The HA equation

![HA Equation Diagram]

The RAS features of HP Integrity Superdome can be classified as either those that address failure avoidance (keep it running) or those that enable quick/accurate fault recovery (fix it fast). HP reliability and availability designs largely contribute to “keep it running” while its serviceability designs are focused on “fix it fast.”

Fault management and fault tolerance

Fault management is the foundation for availability. It is also the means by which we can “fix it fast”. Throughout this paper we will see how the hardware and operating system cooperate to achieve both goals through proactive fault management and serviceability features.

Our fault management designers use industry-leading methods to proactively identify failure modes and address them without causing downtime. This paper will demonstrate those methods. The essence of the HP fault management philosophy is to be proactive in fault identification and recovery so that end-user downtime is minimized.

System-level reliability and availability

Obviously, it is most desirable to avoid downtime events from occurring at all. Fast fault recovery is okay as a safety net, but it should not be used (and is not, in HP systems) as the primary fault management mechanism.

This statement is important because each fault event has some cost associated with it, whether it is a service call, an automated switchover to a backup server, a degradation in performance or capacity, or a system crash/reboot cycle.

Some computer vendors claim that their hardware can be “configured for 100% hardware redundancy,” implying total fault avoidance. What this statement actually means in practice is that extra hardware is available for “swap-in” upon a system crash and reboot. This “extra” hardware, by itself, does nothing to prevent the initial system crash from occurring.
Delivering extreme levels of availability requires that the downtime per year needs to be much less than 1 hour! How can this requirement be met if a system’s “HA strategy” primarily consists of having extra hardware around to deal with problems after the fact? Or by having diagnostics (like IBM’s First Failure Data Capture) deal with the problem AFTER the damage has already been done?

The designers of HP Integrity Superdome understand the components that build high availability, and have delivered the highest levels of availability in this server.

**Figure 3.** Reliability/resiliency is the base upon which all other features are built

Figure 4. HP Integrity Superdome RAS features at a glance

HP Integrity Superdome has a significantly hardened design over other systems in its class, with capabilities that are field demonstrated to be highly reliable. Many customers have reported significantly lower hardware failure rates with HP systems than with competitive systems due to these important resiliency features.
In terms of the hardware, HP Integrity Superdome delivers HA features and processes that specifically address each major functional area in a computer system: memory, CPU, I/O, fabric (crossbar), and cabinet infrastructure. Each of these areas is discussed in detail.

Memory—dynamic memory resiliency

The primary cause of server hardware failures is, by far, faults in main memory. Therefore, it is vitally important to have a hardened memory system. HP has studied the causes of memory system failures and has designed HP Integrity Superdome to be resilient to these types of errors.

There are 4 specific leadership features that together provide the most reliable memory system in the industry. In tandem, these features are called Dynamic Memory Resiliency (DMR).

1. **HP memory “chip spare”—why you can’t live without it**

   The main (~95%) cause of memory failures are dynamic random access memory (DRAM) faults.

   The only way to deal with DRAM faults effectively is to implement resiliency schemes that can withstand the failure of not only just one bit in a DRAM, but also multiple (or all) bits in a DRAM. It has been determined that memory systems with this type of protection fail at a rate of about two orders of magnitude less than those without the feature.

   This scheme is sometimes called “chip-kill” in the industry. “Chip-spare” is the term used by HP, since it more accurately portrays the fact that the memory chips can be thought of as being redundant, with N+1 DRAMs per set of 4 DIMMs.

   Some other vendors deal with multi-bit SDRAM failures by accepting the fact that they will occur. That is, a scheme is used that supports failure detection, but not correction. This scheme, while it may be acceptable in low-end markets, is a dangerous choice for those customers that are betting their business on not having any downtime. *High-end systems based upon this corner cutting are at high risk to fail due to memory problems.*

   **Note that this problem will still plague the newest Sun servers (Sun Fire) because of the failure to implement “chip-kill correct”.*

   HP Integrity Superdome has implemented a main memory architecture that is resilient to errors that affect multiple bits in an SDRAM.

   The memory subsystem design is such that a single DRAM chip does not contribute more than 1 bit to each ECC word. Each main memory access results in 576 bits being read, 4 bits each from 144 DRAMs. The 576 bits are divided into 4 separate ECC domains, with each DRAM contributing only 1 bit to each ECC domain. Each ECC domain can correct 1 bit in error. Therefore, the only way to get a multiple bit memory error from DRAMS is if more than one DRAM failed at the same time, which has a statistical probability of near zero.
The system is also resilient to any cosmic ray or alpha particle strike because, at the most, these failure modes can only affect multiple bits in a single SDRAM. These types of failures are also avoided with this architecture, again since no SDRAM contributes more than 1 bit to an ECC domain.

HP Integrity Superdome is completely resilient to all SDRAM failures, regardless of the number of bits involved in the fault condition. This nearly eliminates memory failures as a source of system errors.

“Chip-spare” is available on any OS running on any partition.

2. **Dynamic page de-allocation (DPD)**

It is possible to have single bits in a DRAM “go bad” (fail hard) during the life of a computer system. It is advantageous to map this location out of main memory, as a persistent single bit memory error is a performance issue.

HP (under HP-UX) has come up with a leadership solution to the single-bit hard-fail problem. If a location in memory is “bad,” that physical page (4k “chunk”) is de-allocated and is replaced with a new page. This physical page de-allocation is persistent across reboots. HP can track as many as 50–3000 bad pages per cell board! These de-allocations occur dynamically, without any OS or application interruption. If a location in memory proves to be “questionable” (i.e., exhibits persistent errors), that memory will be de-allocated online, with no customer-visible impact. Given the number of spare pages in a system, it is likely that the failed memory will never have to be replaced over the life of the product, resulting in a significant reduction in planned downtime.

IBM handles this same problem through hardware “bit steering.” This is an expensive and limited method since the number of spare DRAMs is limited, whereas the page de-allocation technique has been proven to be virtually unlimited in terms of the number of spares available.

3. **Hardware memory scrubbing**

HP employs a combination of hardware (HW) and HP-UX based software (SW) memory scrubbing. The scrubbing of memory is required because without it, random single-bit memory errors look to the operating system as though they are persistent hard errors. The HP-UX SW memory scrubber reads/writes all memory locations periodically. The HP-UX SW memory scrubber, however, does not have access to “locked down” pages. (Databases and the OS lock down some memory.) Therefore, a hardware memory scrubber is required for full coverage. Every memory location that has a detectable memory error will be rewritten with the correct data (scrubbed). This occurs automatically by the hardware itself. The HP hardware scrubber is a key differentiator and it is not available on most industry-available boxes. The hardware scrubber is available for HP-UX, Linux, and Windows partitions.
Address/control parity protection

HP is the only computer vendor that offers parity checking on the memory address/control bus. This checking is important because a “bit flip” on an address/control line may cause the correct data to get written into the wrong location in memory. Therefore, without parity protection, data corruption could result. Furthermore, this data corruption is very difficult to detect, since there is no way to determine how a specific memory location got the wrong data. (Was it an application error? Disk error? I/O error?)

This protection is available with all operating systems.

HP DMR technologies result in maximum uptime and maximum integrity of main memory, placing HP in the leadership position in the industry.

CPU—dynamic processor resiliency

The CPU caches in HP Integrity Superdome are fully protected from single-bit hard errors and random soft errors generated from cosmic rays or other intermittent error generation sources. This is done either through ECC or error handler–based recovery signaled by a parity error. Some systems in the same class are not similarly protected, resulting in errors that are hard to debug and, in many cases, are blamed on the customer environment. It is also important to note that the HP CPU has been developed with a cache layout that significantly reduces the chance of a multi-bit error due to a random cosmic ray strike. This is not true of all industry-available CPUs.

Less resilient competitors’ architectures will be (and have been) plagued with problems.

HP builds on this cache error protection through Dynamic Processor Resiliency (DPR), which is available with HP-UX. DPR is the system’s ability to de-allocate (online) those CPUs that are exhibiting an unacceptable number of correctable cache errors. CPUs are de-configured if the number of corrected cache errors reaches a specific threshold.

DPR makes the system fully resilient to CPU cache errors, which are a major contributor to system downtime. One side effect of DPR is that the system loses processing power if a CPU is de-configured. This issue can be avoided by configuring the system with extra processing power, either active or passive CPUs using Instant Capacity on Demand (or iCOD).

Another feature of DPR is the ability of the system to de-configure failing CPUs and/or specific cache lines during boot (those that failed self-test), and then continue to boot and run the OS. In most cases, the failing CPU can be restored to full working order, resulting in the avoidance of a field service call.

The CPU bus provides a number of features that increase system reliability/availability. The bus provides parity for address and response signals, and full ECC for the data bus. These features eliminate the possibility of system data corruption, and increase the uptime of the system.

Finally, HP processor caches are built with fewer parts than the competition, resulting in higher base reliability.

I/O

I/O errors are a major cause of HW failures. There are three reasons for this:

1. The number of I/O cards in a typical system is large.
2. In general, I/O cards have a higher failure rate than other system components.
3. I/O cards are exposed to frequent human interaction in the data center.

I/O error avoidance is a difficult engineering problem due to these factors.

HP has designed the following features to address this reliability concern.

Dual-pathed I/O

Dual pathed I/O allows accessibility to a storage device/networking end node through multiple paths. The access can be simultaneous (in an active/active configuration) or streamlined (in an active/passive configuration). Care can be taken to eliminate any SPOFs (single points of failure) between two end points. The system software can automatically detect network/storage link failures and can failover (online) to a standby link. This feature makes the system fault tolerant to any I/O cable and device-side I/O card errors, which are estimated to be at least 90% of all I/O error sources.

I/O card isolation

For further fault isolation and containment, each PCI card resides on its own PCI bus. HP is the only computer vendor to offer this feature. Therefore, all PCI card errors are contained on the card that generated the error, and will not propagate to other I/O cards in the system. In other words, all I/O cards are logically and electrically isolated from all other PCI cards. This significantly improves performance and reduces the likelihood of I/O errors.
Furthermore, there are no I/O card errors than can propagate to another hard partition. (For example, an I/O card hardware/software fault in a Windows partition will not affect an HP-UX partition.) This is not necessarily true of IBM LPARS.

I/O card qualification

HP I/O cards are extensively qualified to work in our servers. This means stringent MTBF goals and full interoperability testing of all I/O cards. No incompatible drivers, no bad pointers, no marginal signal quality.

These I/O HA features have significantly reduced failure incidents due to I/O card failures, a problem that plagues lower-quality servers.

PCI card OLA/OLR

Online addition/replacement of I/O resources is the Dynamic Reconfiguration (DR) feature, which contributes most to lower planned HW downtime. The system hardware uses per-slot power control combined with operating system support for the PCI card OLA feature to allow the addition of a new card without affecting other components or requiring a reboot. This feature enhances the overall high-availability solution for the customer since the system can remain active while an I/O adapter is being added. All the PCI cards (Gigabit Ethernet, Fibre Channel, SCSI, term I/O, etc.) and the corresponding drivers support this feature. The new card added can be configured online and made available for applications to use.

Furthermore, I/O cards can fail over time, resulting in an automatic failover to the secondary path or a loss of a connection to a non-critical device (for those devices that do not warrant dual-path I/O). PCI online replace (OLR) allows a user to repair a failed I/O card online, restoring the system to its initial state without incurring any customer-visible downtime.

Fabric (system crossbar) backplane

The system crossbar provides unprecedented containment between partitions, along with high reliability for single partition systems. This is done by providing high-grade parts for the crossbar chipset, hot-swap and redundant power for the backplane, “spare-wire” recovery in the communication paths between HP Integrity Superdome cells, and, unlike other systems with domains, hardware dedicated to guarding partitions from errant transactions generated on failing partitions.

This is in sharp contrast to Sun domains, in which partitions (domains) are involved in each other’s coherency scheme. Therefore, any failure can theoretically cause multiple domains to crash. Examples of such errors include main memory multi-bit errors and cache errors, just to name two. This has been proven at customer sites.

Furthermore, on Sun systems, if a connector pin breaks in the data path, there will be a persistent single bit error (SBE) at the destination. If a memory SBE occurs on a different bit in the same ECC domain, a multi-bit error will result. Therefore, if the connector pins on the backplane are not dynamically repaired by rebooting the machine into degraded mode, a system crash will occur when a memory SBE shows up at an inappropriate bit.

IBM also has many failure modes that can affect multiple LPARS. There is very little hardware separation between LPARS. Most HW failures will likely result in multiple LPARS being affected, as there is almost no hardware isolation between them.

Cabinet infrastructure

Power infrastructure

The DC-DC converters that power the memory system and the backplane ASICs are fully redundant, reducing downtime associated with power conversion.

Furthermore, HP Integrity Superdome hardware is capable of receiving AC input from two different AC power sources. The objective is to maintain full equipment functionality when operating from power source A and power source B, or A alone, or B alone. This capability is called fault-tolerant power compliance.

For equipment to qualify as being truly fault-tolerant power compliant by the “uptime institute,” it must meet all of the following criteria as initially installed and as ultimately used in operation:

- If either one of two AC power sources fails or is out of tolerance, the equipment must still be able to start up or continue uninterrupted operation with no loss of data or reduction in hardware functionality, performance, capacity, or cooling.
- After the return of either AC power source from a failed or out-of-tolerance condition during which acceptable power was continuously available from the other AC power source, the equipment will not require a power-down, IPL, or human intervention to restore data, hardware functionality, performance, or capacity.
• The first or second AC power source may fail one second after the return of the first or second AC power source from a lost or out-of-tolerance condition with no loss of data, hardware functionality, performance, capacity, or cooling.

• The two AC power sources can be out of synchronization with each other, having different voltages, frequencies, phase rotations, and phase angles as long as the power characteristics for each separate AC source remain within the range of the manufacturer’s published specifications and tolerances.

• Both AC power inputs will terminate within the manufacturer’s equipment. Internal or external active input switching devices (e.g., static transfer switches) are not acceptable.

• A fault inside the manufacturer’s equipment that results in the failure of one AC power source shall not be transferred to the second AC power source, causing it to also fail.

• With both AC power inputs available, the power provided by each of the two internal power trains will be 50% ± 10% of the power output for the supply.

• An external software alarm must be provided via the equipment’s software or the host’s operating system when an AC power source is lost or is outside the manufacturer’s published tolerances and when the abnormal condition is corrected.

The design of the individual bulk power supplies (BPS) and the configuration of the power interconnect in HP Integrity Superdome meets the conditions listed above for fault-tolerant power compliance.

**Cooling infrastructure**

All fans in the system (i.e., the system blowers and the fans for the I/O card cages) are fully redundant and hot-swappable.

**Management processor (MP)**

The management processor acts as a centralized place to manage partitions. It handles console management, error code storage, partition configuration, etc. The MP is designed in such a way that a failure of the MP will not cause any partitions to crash nor prevent any partitions from booting or rebooting. Furthermore, the MP can be replaced online, resulting in no incurred downtime for an MP failure. These fault resiliency and serviceability features are industry leadership.

**Other dynamic hardware features**

**Instant Capacity on Demand (iCOD) through HP-UX**

With HP iCOD solutions, HP Integrity Superdome servers can be fully populated with high-performance CPUs at a significantly lower cost. These additional CPUs can then be activated instantly with a simple command, providing immediate increases in processing power to accommodate application traffic demands.

HP iCOD is also a high-availability feature. In the unlikely event that a CPU fails, the HP system will automatically replace the failed CPU on the cell board at no additional charge—without rebooting. In online mode, the iCOD CPU brings the system back to full performance and capacity levels, reducing downtime and ensuring no degradation in performance.

iCOD is a means to add/remove CPUs to/from a partition without worrying about the following:

• Interleaved memory
• Application locked memory
• Server switchovers due to false failures
• Physical handling of CPU/memory boards
• Rebooting

HP iCOD is a true way to reduce planned downtime for HW upgrades.

The Sun version of “dynamic domains” has the following limitations:

• Any of Sun’s Dynamic Reconfiguration (DR) activity requires that the database be shut down, making applications unavailable during the process.

• Sun’s DR cannot be used in combination with memory interleaving across system boards, which reduces maximum performance. Sun customers have to choose between good system performance or DR functionality, but cannot get both at the same time!

• Sun’s DR is not supported in combination with Sun Cluster failover. Since the system halts during a DR operation, Sun Cluster considers this system to be failing and starts a failover procedure to another system. Sun
customers have to choose between a true multi-system, high-availability solution and the use of DR, but cannot get both at the same time!

- Sun’s DR conflicts with Intimate Shared Memory (ISM) used by demanding applications.
  To improve performance, most memory-intensive applications, like databases, make use of the Intimate Shared Memory (ISM) capability in the E10000. Most applications using ISM do not allow dynamic addition or removal of their shared memory allocation. Using memory-intensive applications with ISM (like large databases) and making the most efficient use of partitions prevents the use of DR.
- For Sun, deactivating/moving a system board with full memory can take 15 minutes (backup and rearrange memory contents). All activities in the affected partitions(s) have to be paused during that time. (To compensate, Sun introduced TurboDR boards with just CPUs, no memory.)

These limitations make Sun’s DR unusable in any practical mission-critical configuration. It certainly does nothing to improve system availability. It is important to note that Sun’s DR does nothing to reduce the system crash rate (in other words, Sun’s DR does not prevent system crashes).

Expected HP Integrity Superdome availability

No other computer vendor has a section such as this in any customer-available materials. This is either because (1) these vendors have no idea how their features affect system availability, or (2) they are afraid of publishing the results.

HP is not afraid to discuss system availability because HP understands the elements involved in the HA value chain.

Expected (or average) system availability refers to the expected availability of one or more HP Integrity Superdome servers taken together with a large xp512 data storage array. The expected availability quoted below takes into account unplanned hardware and operating system interruptions that would be experienced by an end user. In addition to the recovery activities needed to restore the system to an operating system prompt, additional recovery activities, such as database recovery, application restart, and end-user re-login, are included in the expected annual downtime results presented below. The results are based on detailed Markov chains that are unique to each of the HP Integrity Superdome servers and system configurations modeled. The configurations that have been modeled include a) single server with two internal partitions running Serviceguard clustering software, and b) two separate servers running Serviceguard clustering software. Results have been developed for clusters where the servers are in active/hot standby mode and also active/active mode. All configurations are assumed to have fast database recovery software in operation. For example, referring to the last row in Table 1, for two HP Integrity Superdome servers in a two-node Serviceguard cluster with one node acting as a hot standby, the expected annual downtime is 0.49 hours (or 29.6 minutes), and the corresponding expected system availability is 99.9944%.

Table 1. HP Integrity Superdome availability modeling results
The steady state availability and expected annual downtime results are due to unplanned hardware and operating system interruptions, and include the associated database recovery time, application recovery time, and end-user re-login time. Fast database recovery and clustering software are assumed to be operating. Each server is configured with 64 processors and 64 GB of memory.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Availability</th>
<th>Downtime (hrs.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single server, 2 partition active/active</td>
<td>99.9873%</td>
<td>1.11</td>
</tr>
<tr>
<td>Single server, 2 partition active/hot standby</td>
<td>99.9923%</td>
<td>0.67</td>
</tr>
<tr>
<td>2 servers, 2 node active/active</td>
<td>99.9864%</td>
<td>1.19</td>
</tr>
<tr>
<td>2 servers, 2 node active/hot standby</td>
<td>99.9944%</td>
<td>0.49</td>
</tr>
</tbody>
</table>

Note: the results in Table 1 reflect 64-way configurations. Smaller configurations will result in even higher availability.

HP-UX reliability and availability features

HP-UX is setting new standards in reliability. Customer-reported defects have decreased 80% over the previous release, which was considered to be among the most reliable operating systems in the industry.

Customers are also very happy with HP-UX, with more than 70% of survey respondents indicating that they were “very satisfied” (the highest ranking) with the operating system software. World-class is considered to be more than 50%.
The main reason for the satisfaction is reliability and uptime, cited by 60% of the respondents as the number one reason for their satisfaction with HP-UX.

Reliability and high uptime are the critical design considerations for HP-UX. All SW components must pass stringent test suites before they can be integrated into the mainline code. Once integrated, the operating system is tested/verified by running it on large configurations using customer applications. This entire SW stack goes through significant stress testing before HP-UX can be released.

“Creating failure avoidance of Web-enabled computing infrastructures through the operating system environment is the first step in achieving single systems availability. Giga uses HP-UX 11i as the best existing example of a UNIX® operating system that has addressed the critical elements of single-system availability from the outset. On the one hand, an Internet-enabled operating system should provide a high degree of single-systems availability; but, on the other hand, it cannot forfeit the flexibility to adjust computing resources on the fly. The collection of functional improvements to HP-UX 11i goes a long way in achieving this balanced objective, making it a sound operating system environment for ISVs targeting the stringent single-system availability demands required by the more commerce-enabled service providers.—HP-UX 11i in Internet Environments (Part 1): On Single Systems Availability, Giga Information Group, August 30, 2000

**Single-system availability** is a recognized strength of HP-UX. HP-UX 11i v2 incorporates many standard features for excellent single-system availability, such as online component replacement and automatic de-allocation of at-risk components. HP-UX 11i v2 also has a complete suite of high-availability products and solutions to ensure continuous application availability while maintaining data integrity.

- nPars or hard partitions allow resource boundaries to be redefined without rebooting complex or non-affected nPartitions in the server
- PCI and PCI-X Doorbell for one-touch online I/O card add or replacement (but not removal); servers supporting the PCI and PCI-X Doorbells will be introduced in Fall 2003
- Faster system memory dump through compressed dump, which speeds up memory dumps for HP-UX 11i in the event of a system crash. The speedup is achieved by compressing small chunks of memory and writing only compressed data to disk. The compression and disk write are done in parallel.
- HP iCOD (Instant Capacity on Demand) and Pay per Use—iCOD for version 2 supports activation and deactivation of iCOD CPUs on an Intel Itanium system; key features of iCOD include the following:
  - Uses portal instead of e-mail to obtain codewords for the activation of additional CPUs (faster and more convenient than e-mail)
- Instantly activates an iCOD CPU without reboot when an already active CPU fails or is proactively deconfigured by DPR because of anticipated failure
- Pay per Use: Pay per Use and iCOD are two separate yet related programs—you don’t need to have iCOD to use PPU. Charges are based on CPU % utilization; uses Smartmeter, a Linux workstation that can monitor up to 200 copies of HP-UX 11i and pushes data to HP every 24 hours

- Dynamically loadable kernel modules for file system (CDFS) enables users to add a CD file system to a running UNIX system without rebooting the system or rebuilding the kernel
- autoFS 2.3 enables more robust automatic mounting of file systems
- Dynamic kernel tunables reduce system reboots. Dynamic kernel tunables are kernel parameters that can be changed by a system administrator without a system reboot; the changes are persistent across reboots. HP-UX 11i v2 provides seven additional dynamically tunable kernel parameters in 11i v2 for a total of 31 dynamically tunable kernel parameters. It is estimated that the dynamically tunable kernel parameters reduce by 50% the number of reboots caused by kernel parameter modification. New dynamically tunable kernel parameters include dbc_max_pct, dbc_min_pct, nfile, nflocksemmsns, semmni, maxfiles
- Dynamic variable page sizing tuning—Based on application-program heuristics and size, HP-UX dynamically, and by default, selects appropriately large page sizes for each memory object it accommodates. This use of larger pages conserves translation lookaside buffer (TLB) entries and reduces the occurrence of costly TLB misses. This capability improves the performance of many applications, particularly those with large reference sets and large amounts of contiguous memory (e.g., databases).
- Auto port aggregation (APA) allows the grouping of up to four physical Gigabit Ethernet or 32 Fast Ethernet links into one virtual high-bandwidth connection. APA supports true load balancing and failure recovery capabilities and distributes traffic evenly across the aggregated links. APA provides automatic link failure detection and recovery that isolate both the application and the transport from any link failure condition by automatically switching data flows to a backup link in case of an individual link failure. This is achieved by allowing each of the links in the “failover group” (also known as link aggregation) to appear as one logical link to the network layer and above.
  Note: APA is not part of the HP-UX 11i v2 release but will be available for Web download in the second half of 2003.
- Mass storage I/O multipathing—Automatic failover and load balancing of I/O when there are multiple paths between the storage host bus adapter and the target I/O device

Serviceability and fault management

Fault management

Fault management is any action taken (preventive, reactive, proactive, or instantaneous) to detect and respond to an unplanned disruption in system availability. As discussed in the previous pages, fault management starts with the quality, the design, and the engineering of every HP server.
In an adaptive enterprise, the built-in product fundamentals are created with much of fault management in mind. It contributes to continuous and secure operation, dynamic resource optimization, and automated and intelligent management. It is the solution base that enables self-healing and platform management. It is not a new concept, nor a new initiative; it is simply and will always be fundamental to HP server designs. With the advent of the Intel Itanium Processor Family, HP extends this fundamental design, enabling this offering for Windows and Linux alike. The total fault management offering translates directly into the following four important customer values:

**Lower risk of downtime due to faults**
- Hardware validation and burn-in tools designed to screen out potential component failures
- Self-healing and highly reliable hardware

**Minimized downtime required to recover from faults**
- Intuitive tools
- Unsurpassed coverage breadth and depth for problem detection and isolation
- Clear and accurate recommended actions for problem resolution included in reported events so that cross referencing with hardcopy guides is not necessary
- Exercisers for intermittent and performance degradation problems
- Verifiers to ensure repair success
- Ease and speed to physical repair

**Problem resolution is easy and low cost; lower TCO**
- Better than an easy install, the tools are preinstalled
- Easy to integrate with the existing infrastructure, whether it is HP OpenView, IBM Tivoli, or some other enterprise management application
- In the event that HP completely manages your environment, the fault management tools become the underlying essentials that extend the capabilities of High Availability Observatory (HAO) and Instant Support Enterprise Edition (ISEE) support services.
- The fault management applications are designed to be intuitive and effective; the user-friendly event descriptions make the problem determination tools easy to use and comprehend
- The management processor also serves as a remote fault management tool providing an out-of-band method to troubleshoot or manage your HP server
- Service access, fewer steps for hardware replacement or repair
Fault tolerant and fault containment designs further ease the repair process.

**Improved total customer experience**
The HP total customer experience is rounded out by making this aspect of the usage phase:
- Simple
- A consistent experience, regardless of the operating system residing on the HP Integrity Superdome hardware

**Serviceability**
The days have passed where serviceability was thought of only in the context of part swapping; serviceability is the whole solution that enables effective problem response, recovery, and resolution. Not unlike the other RAS components, serviceability is made of tools, processes, and hardware designs that ultimately contribute to system availability and determine TCO.

Our serviceability strategy is simple: Fix it fast. Problem resolution is made quicker, easier, and more precise. We conscientiously engineer solutions for maximizing uptime when faults occur and even for instances when faults require hardware replacement to take place.

Figure 8 shows serviceability in its reactive fault recovery space of fault management. However, we will review some of the proactive “keep it running” aspects, providing more detail about the proactive tools themselves.

---

**Figure 8. HP proactive and reactive fault management**

**HP proactive fault management = fault avoidance**

**Keep it running**

- Preventive design
  - Design for reliability and availability
- Proactive tools
  - Detection
  - Isolation
  - Correction
  - Reporting
- Instant remedy solutions
  - Retain capacity

**HP reactive fault management = fault recovery**

**Fix it fast**

- Design
  - Design for availability and serviceability
- Expert tools
  - Analysis
  - Diagnosis
  - Firmware update
  - Verification
- Supportability solutions
  - Expert resources
  - Training
  - Documentation
  - Integrated service

---

727
Proactive fault management

Preventive hardware design
Fault management starts by working with hardware and OS designers to create hardware and software capabilities and instrumentation points that provide the ability to detect and isolate system anomalies at both the manufacturing level and the end-user production environment. The HP Integrity Superdome embodies the latest and foremost of HP fault management to ensure maximum uptime in your high-availability environment. Much of this fault-avoidance design has already been described in the reliability and availability sections. The following sections discuss some additional capabilities involving the serviceability and fault recovery of the HP Integrity Superdome.

HP-UX proactive tools
While much of the proactive fault management space is gracefully handled by the preventive hardware designs, there are also the tools that monitor, detect, and report ensuing faults. The monitoring tools also have the ability to take corrective action before an unplanned downtime event occurs. These monitoring tools are part of HP-UX EMS.

HP-UX EMS
The Event Monitoring Service (EMS) is made up of three primary components: the target and client applications, the resource monitors, and the Event Monitoring Service framework itself. Client applications are the applications used to configure the monitors. Target applications are the end-user interfaces where notifications are sent. The EMS framework contains the APIs, registrar, and resource dictionary.

Resource monitors
Resource monitors include hardware monitors, software monitors, and optional high-availability monitors. Monitors can also be referred to as agents or providers. Resource monitors are responsible for the detection, isolation, and reporting of system faults or impending failures. Notification is available to the system console, e-mail, pager, logs (text log and/or syslog), HP Support Services, and enterprise management platforms.
Hardware monitors are installed with the base operating system and cover both core system components and peripheral devices. These are native EMS monitors and they include CPU, memory, chassis, fans, system bus, temperature, disk arrays, SCSI devices and enclosures, Fibre Channel devices, and power supplies. The monitors perform subsystem log tracking, event correlation to the most suspect FRU, predictive analysis to determine likelihood of impending failure, and reporting with failure cause-action statements. In addition, the monitors extend their value by providing isolation and correction capabilities, also referred to in the industry as self-healing. These include online and persistent de-allocation of failed processors (DPR), de-allocation of memory pages, graceful system shutdown upon power failover to UPS, and automatic system restart upon system hang.

Software and high-availability monitors provide even more extensive monitoring capabilities. These monitors cover kernel resources, network, LAN aggregate and failover, database, clusters, etc. For more information on these specific monitors, go to www.docs.hp.com/hpux/ha/index.html.

Management processor
The management processor (MP) is one of two interfaces that HP Integrity Superdome employs for service and console. The MP is also another means for monitoring the health of the system. One clear advantage of the MP is its out-of-band access, acting independently of both the operating system and the payload LAN. Sometimes referred to as “extended fault management,” the MP is capable of remote power control and environmental monitoring of the fans, temperature, and power supplies (cabinet, cells, and I/O chassis), display of system configuration, and configuration of the MP itself. Users can connect to partition consoles, display server and partition state, reset partitions, view archived and live logs, and (with over 40 available commands) perform many other platform management capabilities. The MP protects the system from unauthorized use of these functions by authenticating users, assigning them role-based capabilities, and by offering secure (SSL-based) access using secure Embedded Web Console.

The management processor also provides a Virtual Front Panel (VFP), a real-time display of each partition’s boot status and activity. The VFP is similar to the LCD display found on many single partition servers, providing the following types of information: progress status of cells or partitions through boot sequence, the operating state of each cell or partition, and any errors detected and flagged during boot process.

The MP was designed to monitor and control system availability. It was also designed so that in the event of an MP failure, the MP itself did not detract from system availability. Therefore, it does not pose a single point of failure and it can be reset or replaced without impact to the remainder of the system.

Support management station
The support management station (SMS) is a Windows-based system that provides a service and console interface for HP Integrity Superdome. SMS provides methods for performing low-level diagnostics, upgrading system firmware components, accessing various event logs, and performing other service tasks. Low-level diagnostics are stored and run from the SMS. These low-level diagnostics are called scan tests and are IEEE 1149.1 compliant boundary scan tests. Scan tests have the capability to diagnose board or chipset faults down to the failing connection or gate by inserting bit patterns into registers within the systems, shifting the bit patterns, and comparing the results with expected results. This enables pinpointing a failing module with extreme accuracy.

The SMS makes access to and from the system more flexible, secure, and comprehensive. Connections to and from the SMS can be either modem or LAN. SMS is advantageous for providing access and support management to a group of servers—up to 16 HP Integrity Superdomes—from a single point.

Reactive fault management
Serviceability design
HP continues its commitment to design features that maximize system uptime, even during system servicing. These are features aimed at reducing the time to upgrade, diagnose, and repair component failures. Designs such as hot-swap, hot-plug, and innovative error containment technologies have been implemented throughout the HP Integrity Superdome server so that addition or replacement of components, coupled with industry-leading tools both eases and quickens the time to repair, all while the system continues to run. The serviceability of the HP Integrity Superdome is made simple, and access and removal of any field replaceable unit (FRU) can be done quickly and easily.

From a fault management perspective, the Table 2 lists preventive designs that contribute to continuous single-system high-availability and serviceability designs that enable simple servicing of a highly complex enterprise-level system.
Table 2. HP Integrity Superdome Hardware Serviceability design

<table>
<thead>
<tr>
<th>Hardware components</th>
<th>Redundant (N+1)</th>
<th>Hot-swap</th>
<th>OLAR</th>
<th>Hot-spare</th>
<th>Fault containment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air intake filters</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fans</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cabinet blowers</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulk power, AC-DC converters</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backplane power, DC-DC converter</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC power cords</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell board power, DC-DC converter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(power bricks)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management processor</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td></td>
<td></td>
<td>X²</td>
<td>X²</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td></td>
<td>X³</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell boards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCSI storage adapters</td>
<td></td>
<td>X⁴</td>
<td></td>
<td>X⁴</td>
<td></td>
</tr>
<tr>
<td>Fibre Channel adapters</td>
<td></td>
<td>X⁴</td>
<td></td>
<td>X⁴</td>
<td></td>
</tr>
<tr>
<td>LAN adapters</td>
<td></td>
<td>X⁴</td>
<td></td>
<td>X⁴</td>
<td></td>
</tr>
</tbody>
</table>

1 The optional iCOD feature enables CPU failover. See the “DPR” and “iCOD” sections.

2 Cell board and components residing on cell board (CPU, memory, power bricks) can be replaced while system remains online, only requiring shutdown of nPar associated with that cell. All other non-associated nPars will remain online. This is made possible by the exclusive HP system crossbar. See “Fabric” section.

3 Chip-spare, also widely referred to as Chip-kill. See “Memory availability” section.

4 Enabled by optional multi-path for networking and storage, i.e., APA, mass storage I/O multipathing, etc.

5 Made possible by dedicated PCI slots. See “I/O card isolation” section.

Redundancy and hot-swap
To enhance uptime, the HP family of partitionable Intel Itanium Processor Family servers has many redundant features. Redundancy is defined as designing in an extra unit so that if one unit were to fail, there are still sufficient units functioning to keep the system running without degradation. Redundancy is also referred to as N+1. Redundant units include fans, blowers, bulk power supplies, and, in the case of the HP Integrity Superdome family, backplane power boards, AC power cords, and cell power DC-DC converters. Redundancy is also achieved by providing multiple paths to devices. This feature, called dual-path I/O, is covered in the availability section. Lastly, HP memory technology also features redundancy without incurring an additional and substantial cost to the server that you may find in other vendors’ solutions.

Not all redundant components are hot-swappable, or vice versa. See Table 2 for actual attributes. An item is defined as hot-swappable if it can be added to or removed from a cabinet while the cabinet remains operational and requires no software intervention, such as bulk power supplies, cabinet blowers, and I/O fans.

Hot-plug and OLAR
An item is hot-pluggable if it can be added to or removed from a cabinet while the cabinet remains operational but requires software intervention to do the operation. Hot-pluggable is also referred to as OLAR.

Hot-spare
Another hot feature that enables instant servicing is hot-sparing. An item is a hot-spare if it resides in a system and serves to automatically replace a failed device or component without any user intervention. Hot-sparing is typical in storage array environments, yet HP has had an industry-proven hot-sparing CPU solution, referred to as iCOD. This has been discussed at greater detail in the availability section.

Fault containment
The HP Integrity Superdome truly exploits the error-containment designs that were discussed in the availability/fabric section. The benefits are twofold: true fault containment and concurrent serviceability. A significant advantage with the HP partitioning solution is that failures can be isolated to a partition and can then be contained to the associated cells. For systems implementing a partitioning schema, this means a failing part can be replaced without affecting the availability of the other partitions currently in use.
Accessibility

In addition to the design implementations mentioned above, design for accessibility is generally applied to all components to contribute to the speed and ease of HP Integrity Superdome servicing. In the modern data center, HP realizes that floor space is at a premium. Servers are arranged in long rows, one rack of equipment butted up against the next. The interruption to a data center having to move racks for side access to a cabinet in the middle of a row would be catastrophic. For this environment, HP has designed its systems to be serviceable from the front and rear or extended from the rack in the case of rack-mounted systems.

Moreover, all field replaceable units (FRUs) are easily accessible. The HP Integrity Superdome serviceability design requirements mandate that FRUs cannot be more than three components deep, otherwise referred to as three-step physical FRU access. This means that no more than two levels of parts need to be removed to access any FRU in the entire system. Units that have a high mean time between failure (MTBF) are tactically designed at the third level, where the probability of failure is virtually none.

Problem determination tools

Diagnostics. The HP Integrity Superdome has four types of diagnostic implementations: component built-in self-tests (BIST), power-on self-tests (POST), pre-OS diagnostics, and online diagnostics. Both BIST and POST are industry-standard offerings, while the offline and online diagnostics have been developed to maximize accuracy and effectiveness of problem determination for the HP Integrity Superdome.

Offline Diagnostics Environment (ODE) is the pre-OS diagnostic platform that provides low-level tests for CPUs, memory, crossbar links, I/O links, and peripheral devices. ODE enables users to troubleshoot a system that is running without an operating system or that cannot be tested using the online tools. Integrating ODE with HP e-Diagtools results in a comprehensive resource that allows for verification of correctly functioning hardware, distinguishing between hardware and software problems, and collecting and summarizing precise system information to further aid in troubleshooting.

Support Tools Manager (STM) is the HP online diagnostics that is installed with HP-UX and can run concurrently with the operating system. The online tools provide information for specified devices, verification of connection and operation, diagnosis for error isolation to the FRU level, exercisers for applying stress testing on intermittent failing hardware, and firmware utilities. STM is developed in conjunction with the hardware monitors, completely leveraging architecture and functionality. It differs from monitors in that it executes specific user-invoked tests against a certain targeted portion(s) of the system, while monitors perform proactive detection and reporting of errors. STM can be executed against the local system, a designated remote system, or multiple systems. In addition, STM can be run from a command line interface, a menu-text driven interface, or a graphical user interface.

Analyzers. The HP-UX fault management tools include three types of analyzers: event analysis and correlation, a kernel crash analyzer, and a hardware system crash analyzer.

Event analysis is performed by the EMS hardware monitors. The monitors track events within their own component subsystem and correlate the events to identify the most suspect FRU. In addition, the hardware monitors perform trend analysis to determine the likelihood of any impending failures. The components currently supporting this feature are CPU, memory, disks, fans, temperature, UPS, and the CEC.

There are two types of kernel crash analyzers offered with HP-UX. ADB is a standard UNIX debugger and is available for debugging purposes. HP also offers q4, a much more friendly debug environment that is programmatic and scriptable. It leverages from the HP knowledge base and provides much more of an advantage over ADB.

The Machine Check Abort (MCA) Analyzer is the Intel Itanium Processor Family hardware post-crash analyzer tool. MCAs caused by low-level hardware, such as timeouts, bus errors, etc., are typically analyzed by HP field engineers to determine failure cause and recommended actions. The complete hardware register dump is saved as a binary file, and referred to as a tombstone file that can be uploaded to a separate console or to HP Support for out-of-band post-crash analysis.

HP-UX system management tools

In addition to the fault management tools, HP-UX has a complete set of system management tools that allow management of hundreds (up to 1,024) of servers from both local and remote locations. The system management tools and products provide extensive capabilities for allocating system resources among application loads. Hardware-based partitioning allows multiple copies of HP-UX 11i (as well as Windows and Linux) to exist in a system and allows each of those copies to be tuned for the applications running under that copy.

- HP-UX Partition Management tools (both CLI and GUI) support HP-UX 11i, Windows, and Linux running in separate partitions: the partition management tools in HP-UX 11i v2 run on Itanium 2-based systems, although they can manage partitions on PA-RISC nPartition servers. The two most significant improvements in the HP-UX
11i v2 partition management tools are: 1) remote management and 2) the “Big Picture Views” capability in Partition Manager (the GUI). Remote management allows the partition management tools to be run on a system apart from the complex being managed, and supports managing a complex with none of the partitions booted. The “Big Picture Views” allow system administrators to graphically view and manage the cell and I/O resources and the various partition configurations within or across server cabinets. Additionally, Partition Manager allows management of HP-UX and now Windows and Linux partitions within an Itanium 2–based system environment.

- Service Control Manager 2.0: Web-based multi-system system management of HP-UX and Linux with single sign on, role-based management, and audit logging.
- Native Event Monitoring Service (EMS) and high-availability monitors, including support for both IPv4 and IPv6: EMS is a system monitoring application designed to facilitate real-time monitoring and error detection for HP-UX systems in the enterprise environment. This framework provides centralized management of hardware devices and system resources and provides immediate notification of hardware failures and system status.
- Ignite-UX: Flexible tool for rapidly deploying and recovering HP-UX systems. For HP-UX 11i v2 there are improved software selection capabilities and the ability to configure a security profile at installation time (installation security).
- Software Distributor: Sophisticated toolset for distributing, installing, and updating HP software products.
- HP-UX Workload Manager (WLM) 2.1 now offers Itanium 2–based server support as well as support for PA-RISC–based servers: HP-UX WLM 2.1 includes support for automatic re-allocation of resources between processor sets (pSets) as well as the existing ability to re-allocate CPU resources between PRM groups or vPars. In addition, WLM 2.1 adds a passive mode and a monitoring GUI, and improves Serviceguard and chargeback support. Finally, WLM 2.1 adds support for BEA Weblogic through a new toolkit.

Supportability solutions

The tools previously described can stand alone or can integrate and serve as the underlying foundation that propagates critical system information upwardly into high-availability solutions, enterprise management applications, and remote HP Service/Support offerings. For more information on these value-add solutions, please contact your local HP sales representative.

Figure 10. Supportability integration

Top-to-bottom system fault management
High-availability integration
HP Serviceguard is a “specialized facility for protecting mission-critical applications from a wide variety of hardware and software failures.” The EMS hardware monitors easily integrate with Serviceguard so that the appropriate hardware failover occurs.

Enterprise management integration
Fault notification provided by the hardware monitors can also be managed by today’s common enterprise management applications. Some of these widely known enterprise management tools include HP OpenView, IBM Tivoli, BMC Patrol, CA-TNG, and NetCool. Integration is not limited; it is also possible with other management platforms supporting simple network management protocol (SNMP) or Web-based enterprise management (WBEM).

HP support and service integration
HP Instant Support Enterprise Edition (ISEE) offers a state-of-the-art remote and proactive support platform for customers with an HP support contract. ISEE provides secure and remote hardware event management, execution of hardware diagnostic support scripts, and network access for HP support engineers (advanced configuration only). It can serve to be a common framework through which HP can access, analyze, and monitor the customer’s environment by deploying a wide variety of “customer-valued” support-related services, even across multiple heterogeneous product lines.

Remote hardware event management is achieved by diagnostic software used to monitor hardware status and generate notification events when predetermined conditions are detected. Notification events are forwarded to HP for review and possible action, helping you to identify and minimize potential problems.

Execution of diagnostic scripts are made possible by a diagnostic engine installed on a monitored client capable of remotely executing support scripts that diagnose problems on systems. In addition, system configuration information can be collected for faster problem resolution.

Engineers in HP response centers have the capability to remotely log in to a secure support node to provide remote hardware or software support for faster problem resolution. This capability is offered for “advanced configurations” only.

HP understands your company’s security concerns and has leveraged its experience as a technology leader to make its remote support solution secure. The design of HP ISEE incorporates a number of leading security technologies and standards encryption, authentication, and industry standard security protocols and best practices.

Summary
HP began its commitment with its HP servers to deliver world-class serviceability and fault management capabilities to prevent or quickly resolve every fault every time. These capabilities are fundamental—the very foundation for self-healing systems. With the advent of the Intel Itanium Processor Family, HP extends this fundamental and strives to enable this offering for Windows and Linux alike.
Table 3. Design, technology, and tools that enable effective servicing of the HP Integrity Superdome

<table>
<thead>
<tr>
<th>Serviceability enablers</th>
<th>HP Integrity Superdome</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware design</strong></td>
<td></td>
</tr>
<tr>
<td>Redundancy</td>
<td>Y</td>
</tr>
<tr>
<td>Hotswap</td>
<td>Y</td>
</tr>
<tr>
<td>OLAR</td>
<td>Y</td>
</tr>
<tr>
<td>Fault containment</td>
<td>Y</td>
</tr>
<tr>
<td>Front and rear cabinet access</td>
<td>Y</td>
</tr>
<tr>
<td>Three-step physical FRU access</td>
<td>Y</td>
</tr>
<tr>
<td>Tool-free or single tool torx</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Visual aids</strong></td>
<td></td>
</tr>
<tr>
<td>Exterior LED panel</td>
<td>Y</td>
</tr>
<tr>
<td>Internal I/O LED panel</td>
<td>Y</td>
</tr>
<tr>
<td>Internal cell board LED panel</td>
<td>Y</td>
</tr>
<tr>
<td>Cable connector color coding</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Out-of-band tools</strong></td>
<td></td>
</tr>
<tr>
<td>Management processor</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Offline tools</strong></td>
<td></td>
</tr>
<tr>
<td>Inventory collection</td>
<td>Y</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Y</td>
</tr>
<tr>
<td>Exercisers</td>
<td>Y</td>
</tr>
<tr>
<td>Firmware update tool</td>
<td>Y</td>
</tr>
<tr>
<td><strong>OS-dependent</strong></td>
<td>HP-UX</td>
</tr>
<tr>
<td>Hot-plug I/O adapters (PCI OLAR)</td>
<td>Y</td>
</tr>
<tr>
<td>Multi-path I/O</td>
<td>Y</td>
</tr>
<tr>
<td>Dynamic processor resilience (DPR + iCOD)</td>
<td>Y</td>
</tr>
<tr>
<td>Online inventory collection</td>
<td>Y</td>
</tr>
<tr>
<td>Online hardware fault monitoring (detection, isolation, reporting)</td>
<td>Y</td>
</tr>
<tr>
<td>Online or concurrent diagnostics</td>
<td>Y</td>
</tr>
<tr>
<td>Crash dump analyzer</td>
<td>Y</td>
</tr>
<tr>
<td>Integrated support solution (hardware-specific)</td>
<td>Y</td>
</tr>
</tbody>
</table>

Figure 11. Obtaining HP fault management tools

Tools

<table>
<thead>
<tr>
<th>Ignited with operating environment</th>
<th>SupportPlus CD quarterly releases</th>
<th>Downloadable from Web</th>
<th>HP service personnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMS monitors</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Offline diagnostics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Support tools manager</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hardware crash analyzers</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Software crash analyzers</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Web download: www.software.hp.com/

Documentation

<table>
<thead>
<tr>
<th>Bundled hardcopy</th>
<th>Manual pages</th>
<th>SupportPlus CD</th>
<th>Downloadable from Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Web documentation: http://docs.hp.com
HP-UX 11i release names and release identifiers

With HP-UX 11i, HP delivers a highly available, secure, and manageable operating system that meets the demands of end-to-end Internet-critical computing. HP-UX 11i supports enterprise, mission-critical, and technical computing environments. HP-UX 11i is available on both PA-RISC systems and Itanium-based systems.

Each HP-UX 11i release has an associated release name and release identifier. The `uname (1)` command with the `-r` option returns the release identifier. The following table shows the releases available for HP-UX 11i.

Table 4. HP-UX 11i releases

<table>
<thead>
<tr>
<th>Release name</th>
<th>Release identifier</th>
<th>Supported processor architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX 11i v1</td>
<td>B.11.11</td>
<td>PA-RISC</td>
</tr>
<tr>
<td>HP-UX 11i v1.5</td>
<td>B.11.20</td>
<td>Intel Itanium</td>
</tr>
<tr>
<td>HP-UX 11i v1.6</td>
<td>B.11.22</td>
<td>Intel Itanium</td>
</tr>
<tr>
<td>HP-UX 11i v2</td>
<td>B.11.23</td>
<td>Intel Itanium</td>
</tr>
</tbody>
</table>