White Paper

Server

How SUSE® Manager Helps to Reduce System Downtime

SUSE
We adapt. You succeed.

Introduction

Most corporate businesses have become more and more dependent on information systems to support business-critical applications. When systems go down, businesses become less competitive and lose revenue.

Not surprisingly, zero downtime is a goal of many IT organizations. There are many reasons why systems can fail: hardware, network, power supply, system software, application software, failure to apply patches and updates in a timely manner, etc. Fortunately, there are techniques and technologies to reduce downtime.

A Closer Look at Downtime

Downtime, planned or unplanned, is the time during which a system is not functioning correctly and is unavailable to users. Planned downtime is scheduled in advance for activities such as regular maintenance and system updates, software patches and upgrades that might require a system reboot, etc. Some actions traditionally included in planned downtime, such as patching, can be performed with reduced downtime by choosing the appropriate systems management tools.

Unplanned downtime is due to unexpected system or environmental failures. Typical causes of unplanned downtime include:

- *Human errors*
- *Earthquakes, fires, floods, hurricanes, etc.*
- *Power outages*
- *Hardware failures (failed CPU or memory components)*
- *External storage device failures*
- *Network failures*
- *Software failures, possibly due to failure to perform patching and updating in a timely manner and/or errors introduced during product development*
- *Lack of appropriate hardware/software for monitoring and detecting errors*
- *Cooling equipment failures*
- *Security breaches by intruders*

According to Dunn & Bradstreet (**www.strategiccompanies.com/pdfs/Assessing%20the%20Financial%20Impact%20of%20Downtime.pdf**), 59 percent of Fortune 500 companies experience a minimum of 1.6 hours of downtime per week. For medium and large companies, this can amount to millions of dollars in labor costs alone due to loss of productivity. When the total expected loss for an hour of downtime for a particular system is calculated (when all factors contributing to loss are included), the potential loss from downtime shocks most people the first time they see it.

To grasp how difficult it is to avoid downtime, all of the following system components must work correctly or be repaired automatically (with no downtime):

- *Power supplies*
- *CPUs and memory in all relevant servers*
- *Operating systems running all participating systems*
- *Server disk drives and other relevant storage devices*
- *DBMSs on the servers*
- *Application software*
- *Network switches, routers and connections*

Systems that have truly continuous availability are rare and expensive. Most have carefully implemented designs such as fault-tolerant systems that eliminate single

points of failure and allow online hardware, network, operating system, middleware, and application upgrades and component replacements. These systems accomplish continuous availability via highly redundant (usually dual) components.

How You Can Move toward Zero Downtime

No single technology can move you toward zero system downtime. Minimally, it requires both hardware and software technologies across various system levels. The desired processes and technologies include:

- *Automating many of the processes used to make updates, perform patching, etc.*
- *Using hardware with good RAS (reliability, availability, and serviceability) capabilities such as the new x86-based processors produced by AMD and Intel and x86-based servers from vendors such as HP and Dell that provide memory board/physical CPU hot add/remove (replace memory boards or CPUs without shutting down a system), parity checking and error-correcting code, etc.*
- *Using a Linux operating system that is integrated with the new x86 hardware like the hardware/OS integration of RISC/UNIX platforms and cooperates with the underlying hardware to reduce unplanned downtime*
- *Using high availability clustering software to mask individual server availability issues*
- *Utilizing carefully selected systems management tools*

In short, the need to automate as many of the processes as possible to provide updates, patches, move from a failed hardware component to a new one, etc. to reduce downtime is overwhelming. It is unlikely that an engineer involved in restoring a system that has failed can do so in less than 5.26 minutes (five 9s availability). The engineer gets notified of the failure, displays alert information to others, opens a trouble ticket, diagnoses the root cause, determines a fix, installs the fix and restarts the system. Even for simple failures, these steps are not likely to be performed in 5.26 minutes.

Automation combined with monitoring may resolve issues that could result in downtime by either resolving them automatically before they actually occur or quickly notifying administrators of the potential issue. Automation can also address complex external regulations and standards requirements without human intervention.

SUSE has taken advantage of the features that AMD and Intel have placed in their x86 processors and that server hardware vendors have included in their new x86-based servers. SUSE has tightly integrated its SUSE® Linux Enterprise Server operating system with this newer x86 hardware to ensure that it is cooperating with the hardware to produce systems with RAS comparable to and sometimes exceeding the RAS of RISC/UNIX platforms, moving customers closer and closer to zero downtime.

SUSE has gone beyond tightly integrating SUSE Linux Enterprise Server with new x86 hardware platforms with its development of SUSE Manager management software. SUSE Manager manages SUSE Linux Enterprise Server, Red Hat Enterprise Linux and CentOS platforms from a single console. SUSE Manager also interoperates with Microsoft System Center, enabling Windows system administrators to view server health information and perform both Windows and Linux patching duties via a single console.

Using SUSE Manager to Reduce Downtime

Well-designed systems management tools can reduce downtime. A research report by IDC[1] indicates that well-targeted technology upgrades, such as upgrading to new servers with improved RAS capabilities coupled with a program to improve systems management tools, can reduce the risk of system downtime, sometimes by as much as 85 percent. IDC also indicates that providing consistent use of software management tools to monitor and manage various maintenance processes, such as updating and patching, can reduce downtime, primarily planned downtime, by as much as 65 percent (assuming that other factors that can reduce downtime are held constant).

As much as 90 percent of downtime in companies is planned, leaving only 10 percent of downtime unplanned. Reducing

1 *IDC Document #219697, Reducing Downtime and Business Loss: Addressing Business Risk with Effective Technology*

the amount of planned downtime should be a main concern of IT and vendors producing system management tools.

SUSE Manager can be used to reduce planned and unplanned downtime. It has already been found to be useful in helping to satisfy regulatory compliance requirements and reducing the time to perform Linux server patch management by eliminating troublesome manual patching errors.

SUSE Manager provides a broad set of features/services (listed below) for managing both physical and virtual infrastructures to reduce downtime. Most of these features/services are for reducing planned downtime, but use of these features/services can decrease unplanned time as well.

SUSE Manager orchestrates updating and patching Linux systems, managing when the downtime will occur so that these activities will cause the least amount of interruption from planned downtime. This includes scheduling patching and updating systems when critical business applications are not running.

SUSE Manager's configuration management feature can be used to make sure that selected server configurations are the same on all the servers in a group. This helps you ensure that security updates and patches have been applied to all the servers that require them, enabling you to determine if a server has the latest updates.

Misconfiguration is one of the most common reasons for system failure/downtime. A classical example is services that were not added to the run level in which they should run. When this occurs, the administrator manually starts the services and everything looks fine. However, if a simple power outage triggers a hardware reboot, this leads to complete failure because the service does not automatically come up. Incidents like this can be prevented by carefully planning configuration and centrally managing any changes.

SUSE Manager uses health monitoring to watch the state of a system over time to identify systems that are running out of resources, such as memory, which can lead to system failures. It provides both real-time and historical state-change information, as well as specific metrics. The administrator is notified of failures immediately and warned of performance degradation before it becomes critical. SUSE Manager also collects information necessary to conduct capacity planning and event correlation. For instance, the results of a probe recording CPU usage across systems proves invaluable in balancing loads on those systems.

SUSE Manager ensures that you do not introduce human errors when patching and updating systems by enabling you to work in an organized manner. You can define when patching happens and define who is going to perform it. With SUSE Manager, you can do all of your patching and updating as well as test the environment and roll it out to production.

SUSE Manager helps system administrators become aware of what needs to be patched, makes sure that you apply patches and helps create a schedule for patching. It can tell you when a system needs to be rebooted, and it provides the capability for you to schedule rebooting and patching downtime in maintenance windows that do not interfere with running production programs.

SUSE Manager can help prevent unplanned downtime by ensuring that patches and updates including security updates, are applied in a timely fashion and in an appropriate time period. These patches and updates may prevent unplanned downtime by removing an error that could cause an application or operating system to fail later. Similarly, patches and updates that remove security vulnerabilities could prevent an intruder from bringing down the system later. In short, patches and updates applied today prevent unplanned downtime tomorrow.

SUSE Manager provides several features for reducing downtime, including:

- *Automating patch management, thus removing error-prone manual procedures*
- *Automating service pack updates by providing the option of updating an existing system to a new service pack without completely re-installing it; no manual installation is needed*
- *Scheduling patch updates and bug fixes in low-risk production hours to avoid unplanned downtime during business-critical peak hours*
- *Allowing administrators to pre-load patches for systems prior to applying them, reducing downtime for patching systems*
- *Reducing the number of unnecessary patches required to patch your systems, lowering downtime*
- *For software updates that require rebooting, such as kernel patches, determining if the system administrator has rebooted; if not, SUSE Manager identifies the systems that need rebooting (Failure to reboot means that the patches that fix potential problems are not applied.)*
- *Providing administrators with information about the cause of various hardware failures through the use of asset management capabilities that automatically track server changes and keep a history of changes. This reduces compliance audit complexity and helps you to track down errors that may cause (or lead to) outages.*
- *Using consistent, template-based provisioning to reduce set-up errors that lead to system failures and unplanned downtime*
- *Utilizing the OpenSCAP approach to maintaining the security of corporate Linux systems*
- *Providing an easy-to-use interface to Common Vulnerability and Exposure (CVE) data, allowing administrators to more easily search for publicly known vulnerabilities and exposing and determining which systems are affected*
- *Using configuration management to avoid configuration drifts that may lead to configuration-related failures*
- *Using health monitoring to identify systems running out of resources that can lead to system failures*

Summary and Real-World Examples

When your systems are unavailable to support critical business applications, development activities and more, your business will become less competitive, lose revenue and experience lower productivity. Without systems management tools that automate updating, patching, etc., such as SUSE Manager, it is nearly impossible for you to move toward zero downtime. A simple manual update that results in an error can make a system unavailable for minutes and even hours.

Most of the system downtime that companies have to deal with is the result of planned downtime. To reduce planned downtime for updating, patching and other planned activities, SUSE Manager helps you schedule planned activities so that downtime is reduced and planned unavailability is minimized. SUSE Manager also focuses on ways to reduce unplanned downtime by ensuring that you make updates and patches in a timely manner. An update installed today may save you unplanned downtime tomorrow.

Rackspace and Delta Lloyd have been using SUSE Manager to reduce downtime and facilitate system management activities. While SUSE Manager's ability to reduce planned and unplanned downtime is an important feature for both companies, its ability to patch multiple Linux platforms from a single console is also an important feature.

When Rackspace[2] needed a provider to help enhance its Fanatical Support to affected customers of its public cloud

2 *Rackspace success story on:* **www.suse.com/success**

offering and a flexible and cost-effective solution that could handle and patch multiple Linux platforms it chose SUSE and SUSE Manager. Rackspace operates data centers on four continents with three of them up and running. SUSE has implemented SUSE Linux Enterprise Server and SUSE Linux Enterprise Server High Availability Extension running SUSE Manager to provide a high availability environment on some of Rackspace's servers.

When the IT organization at financial services provider Delta Lloyd[3] set out to find a lower cost server management tool that would provide a high degree of server availability and security, it selected SUSE Manager. Delta Lloyd chose SUSE Manager to replace Red Hat Network Satellite because of the ability of SUSE Manager to manage both Red Hat and SUSE Linux servers.

For both Rackspace and Delta Lloyd, SUSE Manager was able to ensure high availability while reducing the cost and complexity of high availability in environments with diverse servers.

3 *Delta Lloyd success story on:* **www.suse.com/success**

Contact your local SUSE Solutions Provider, or call SUSE at:

1 800 796 3700 U.S./Canada
1 801 861 4500 Worldwide

SUSE
Maxfeldstrasse 5
90409 Nuremberg
Germany

www.suse.com