Devising A Plan to Improve System Availability

By: Harris kern's Enterprise Computing Institute

In this article we describe how to devise an effective plan to address system availability. You must first understand the *entire* system, and how each component affects overall system availability. By then identifying the *most critical* system components, you can intelligently set priorities. Remember that no matter how insignificant a system component may seem, it can have a profound effect on overall system availability. Once you identify the most critical components, seek ways to improve their *reliability, recoverability, serviceability,* and *manageability*.

Identifying System Components

To improve system availability, first identify all the system components that work together to enable a user's application to run. A chain is only as strong as its weakest link. If your system has one component that is prone to failure, your entire system is prone to failure.

Technology

Most systems can be divided into the following elements:

- **Server -** This is the portion of the system where most data is stored or processed. The server fulfills transaction requests sent to it and sends the results to the requestor of the transaction. For example, in a bank Automated Teller Machine (ATM) system, the host is usually the bank mainframe system, or large server, that manages client bank accounts and transactions.
- **Client** - This is the component that makes a request from the server. In our ATM example, the client is the ATM machine.
- **Network -** This is the component that allows the client to communicate with the server, and vice versa. In our ATM example, the network is typically a combination of a private network, the public telephone network and all associated communication equipment.

For each of these areas, examine all components: hardware, software, environment, processes and procedures, and personnel.

Hardware

Hardware is the physical equipment making up the system. It includes, but is not limited to, the following:

- **Central processing unit** — The device that controls the operation of the computer system or other intelligent equipment
- **Storage devices** — Data repositories, whether permanent or volatile media, such as memory and hard disks

- **Input devices** — Components for receiving commands or data from users or other equipment, for example, keyboards, mice, and serial ports
- **Output devices** — Components for presenting data to the user, such as monitors, speakers, and printers
- **Cables** — Often neglected but crucial to the reliability of any computer system

Software

Software consists of the programs running in the system that enable it to perform its functions, including:

- **Firmware** — Software embedded in hardware, acting as the interface between hardware resources and the operating system. In PCs, this software is also called the Basic Input/Output System (BIOS).
- **Operating system** — Core programs that allow applications to run on a computer without directly interfacing with the computer's hardware components. Common operating systems include Windows, UNIX, Linux, OS/400 and OS/390.
- **Utilities** — Software that performs housekeeping and system control functions. Normally, system administrators or maintenance staffers use these programs.
- **Programming software** — Software that supports the creation of applications, including languages such as C++, Java and COBOL; and development tools such as Microsoft Visual Studio.
- **Applications** — Programs designed to perform user-specified tasks or operations. These programs may be written by the company (in-house applications) or purchased from a software vendor (off-the-shelf or shrink-wrapped software).
- **Middleware** — Programs supporting communication or data exchange between multiple programs or computer systems.

Environment

The Environment covers all the is the external equipment the system needs in order to run:

- **Power** — Including automatic voltage regulators, uninterruptible power supplies, generators, surge suppressors, and lightning arrestors
- **Cooling** — Including air conditioning units and dehumidifiers
- **Floor space** — Including raised flooring and secured access areas

Processes

Processes and procedures are the operational activities needed to run the system. These include, but are not limited to:

- **Activation** — Including power up, system initialization, application startup, and verification of system activation

- **Operation** — Including resource management, input/output control, job control, and network management
- **Systems management** — Including system monitoring and change administration
- **Housekeeping** — Including backup and restore, as well as archiving of data
- **User management** — Including user and security administration
- **Deactivation** — Including application shutdown, system shutdown, and power down

People

People refers to those who interact with the system:

- **Users** — Including both internal and external users
- **System support staff** — Including operators, system administrators, programmers, technical support professionals, and others
- **Vendors and suppliers** — Including electricity vendors, equipment suppliers, telecommunications providers, and others

Addressing Critical Components

After you identify all relevant system components, the next step is to find the *critical* system components, those that represent single points of failure for the system. When these components encounter a problem, the entire system is affected.

Several approaches are available for reducing the risks associated with these critical components:

- **Reduce outage frequency -** Look for ways to prevent outages from happening to that critical component, thereby increasing its reliability.
- **Minimize outage duration -** If outages cannot be entirely avoided, find ways to recover immediately from them, thereby improving recoverability. If recovery is impossible, ensure that the component can be immediately repaired - in other words, improve serviceability.
- **Minimize outage scope -** Minimize the parts of a system that are impacted by an outage.
- **Prevent future outages** - Reduce the potential for users and other external factors to affect system availability, and make it easier to maintain the system's health by addressing its *manageability*.