A Common Monitoring System for Network and Application Services in the Internet.

Motivation

The majority of the Internet network services (DHCP, DNS, E-Mail, etc) have already some form of redundancy mechanism that sets their resilience to a certain level. The resilience level for these services can be satisfactory only if the resilience of the underlying network and supporting computer resources is high enough so the frequency and duration of episodes that make these services unavailable (or performing deficiently) have no discernible effect on the overall quality of service as it is perceived by the users.

One of the most important and common requisites of these redundancy mechanisms is the need for simultaneous installation of mirroring running service elements or secondary servers. These secondary servers are defined on a fixed basis and there is no real automatic substitution of a faulty primary server. Without human intervention, the level of redundancy is diminished every time one of the servers (primary or secondary) becomes unavailable.

Reposition of the redundancy level can only be accomplished with a mixture of planned and improvised procedures that depend heavily on manual/human intervention from the network management staff although network services management applications can help monitoring services and warn in case of unavailability.

Pure server substitution is usually not considered and some services don't rely on secondary servers (like the routing service, for example, which relies on replication of the routing database to all running servers without the use of secondary routing servers).

Sometimes, load balancing is used has an indirect method to implement redundancy but it will also mandate the need of, at least, two running servers at all times, and they will not share exactly the same service databases.

Finally, some services can use complete server replications, although this is usually achieved using a front-end interface (virtual server) that replicates all the interactions between clients and servers.

A Common Redundancy and Backup System for Network and Application Services on the Internet would have an important impact on the current network management activities and practices since it would provide a unique methodology for implementation of redundancy and a backup feature for all these services, eliminating the need for knowledge of several systems and the use of a different software implementation for each service.

Also, this would permit separate development and implementation of the productive functions of the services and the redundancy and replication aspects.

Objectives

The mechanism used for self monitorization (between servers of the same service), or the method these services provide for monitorization through external management systems, is the first component taking action on a redundancy or backup network service system.

Some services do not use or provide any mechanisms for direct verification of their operational status while others rely on specific mechanisms for mutual status verification by the running servers. Either using an active or passive approach, each standard network service or application uses its own fault detection mechanism, although some can share a common strategy.

A common monitorization mechanism should be one of the most important components of a Common Redundancy and Backup System for Network and Application Services on the Internet.

So, the main objectives for this work would be:

- To study and analyze the redundancy mechanisms of all the major TCP/IP network services and applications and to discover common strategies, features and techniques used for monitorization of standard network and application services. This should also lead to the identification of the major limitations of such individualized approaches.

- The core of the research work will have as its main objective the definition of a common, generic strategy that could be adopted (by means of a well defined protocol) by all standard TCP/IP network services and applications, overcoming, at the same time, the vulnerabilities previously identified. This new strategy should be based on state of the art monitorization techniques for TCP/IP networks, supported, or not, on standard protocols, like SNMP.

- The research work should be complemented with the development of a software implementation of a simple prototype monitorization system and integrated with an existing open source network service (for example into DHCP or DNS servers). A variety of tests should then be run on a prepared network environment so to prove that the new monitorization system performs as expected in comparison with the standard monitorization mechanism of that network service.

Supervisor: Bruno Dias, <bruno.dias@di.uminho.pt>
Research Unit: CCTC