Internal Support Agreement

By: Harris Kern's Enterprise Computing Institute

Businesses have enough competition outside the business without having it inside as well. I propose creating an internal service level agreement called an internal support agreement to keep your infrastructure support group and your applications development staff away from each other's throats.

In many of the companies we visit, the applications development staff is located at the division or business-unit level. Unfortunately, the support groups reside in different buildings. How does a centralized IT infrastructure support group provide System Administration services to scattered corporate developers? This and other issues should be clearly defined in an *internal support agreement*.

Of all the battles inside IT, none have been uglier than those between applications development and the infrastructure support organization. Even when development and support were centralized under one organization, there was always finger-pointing. The charter for applications development is to design, develop, and deploy systems into production as quickly as possible. The charter for infrastructure support is to ensure that proper standards, guidelines, and QA testing are adhered to, and that thorough documentation is provided. Most of the issues arose around implementation and support of mission-critical applications. Development would blame Operations for messing up a restart to a system error, or Operations would blame Development for lack of QA or support. There were many other issues of this nature.

As in the mainframe era, developers still want the centralized IT infrastructure staff to support development servers in a limited way for such mundane tasks as backup-and-restore. But today's development servers are a problem for both the development group and infrastructure support. Developers want top-level, "root" or full administrative access to their development machines. This is a problem because owners of root passwords can bypass normal safeguards and unwittingly destabilize a machine in seconds.

On the other hand, developers do need occasional unlimited access to a machine. Denying access makes their jobs more difficult than necessary or even impossible. What to do?

To solve this problem, we devised *joint root authority*. The infrastructure support organization and the two most senior developers will own root access. If developers abuse root privileges, the infrastructure organization will no longer support development servers.

One of the most important pieces of this puzzle is an *internal* Service Level Agreement (SLA) between the infrastructure support staff and the applications development staff. In this document, expectations are clearly outlined for both groups. The following sections show some of the key categories and examples of an internal SLA. When designing an Internal SLA (for supporting a development server) the first area to start with is defining security privileges.

Server Root Authority

Root access to support servers AD0001 and AD0002 in the following example is given to Mr. A and Ms. B. Mr. A and Ms. B are to support/back up each other in case of illness or vacation. If they're both unavailable, you would contact Technical Services.

All changes to a server's root will be audited to provide a trace of root user activity. The following activities are accomplished by Technical Services upon request:

- Kernel changes
- Disk reconfigurations
- Modifications to the root user environment
- Installation of binaries into the system directory structure
- Modification to any network-related configuration files
- Manipulation/modification of any system daemon run at the root level
- Changes to the /etc/rc* files

The following is a partial list of activities that may be accomplished by the applications development root owners:

- Change /etc/exports for mount directories
- Change /etc/fstab
- Add users/groups

Server Availability Hours
The following schedule determines server availability, which is established between Applications Development and the infrastructure support organization.

- 00:00 - 23:59 M, T, W, Thr, and Sun
- 00:00 - 23:00 F
- 03:01 - 23:59 Sat
- 20:00 - 23:59 (once a month for system maintenance, upgrade, and testing, all will be posted through Change Control)

Backups
Full system backups start at 23:00 every Friday, with a total downtime of four hours.
Incremental backups start at 20:00 every Monday – Thursday

Support Responsibility

Services	Group	Types of Services	Hours
System Software	Technical Services	Solaris, Linux, Sybase, installation, upgrade, maintenance	00:00-23:59
System Hardware	Desktop Support	Server, monitor, workstation, installation, maintenance	00:00-23:59

Application	Application Development	Set up applications and perform demonstrations, project file access	08:00-18:00

Server Functions

Server AD0001
This server is the primary development machine to carry the more CPU-intensive workload. Free temporary disk space is available on this machine via UNIX automount. Disk quota is set up for each project. Disk space availability is determined by the scope of the project.

- Solaris
- Linux
- DNS and NIS slave server hostname, IP address, aliases
- Database server (such as home/sybase)
- Free hog disk space via automount (for example, /home/common)

Server AD0002
This machine is used as the pre-production server.

- Solaris
- Linux
- Project files, data, databases (such as /home/hrproj)
- Client's personal files (for example, /home/username)
- Support SunX clients

Special Requests
These are different categories of special requests and their estimated completion times. These changes include investigating whether the proposed change affects other applications on the server. Technical Services notifies the requestor if the request takes longer than the estimated completion time.

Request	**Estimated Completion Time**
Emergency backup and restore	Processed within 4 hours
File maintenance: • Change /etc/experts for mount directories • Change /etc/fstab • Add users/groups • Modifications to fstab, group, add users, change permissions	Processed within 8 hours

Operations request	Up to 2 working days
Backup and restore (UNIX files only)	Up to 2 working days
Solaris kernel	Up to 5 working days for software that requires kernel modification
Database change	Up to 5 working days
Hardware configuration	Up to 5 working days