Desktop-based Network Management

L. Deri
Finsiel S.p.A.
Via Matteucci 34/B
56124 Pisa
Italy
l.deri@finsiel.it

In the management world, the web is considered by many people the best user interface for next generation management systems. This is because the use of the web has several benefits with respect to non web-based management applications such as:

- Web browsers are provided with almost every OS.
- Hypertext facilities can be profitably used for on-line help and documentation.
- Web pages can integrate multiple heterogeneous services and living Java applets.

Beside all these benefits, the use of the web as alternative to platform native applications has shown some limitations such as:

- Limited Operating System Integration
  Contrary to a common belief, the desktop has been web-ised and not the other way round.
- No Scriptability and Task Automation
  HTML is meant for human display and not for batch processing.
- Resource Integration vs. Resource Composition
  The web allows people to easily integrate various resources and Java applications in a HTML page. Resource composition (software composition) instead, allows developers to compose different resources such as software applications and documents, and produce yet another composable resource.

Basically, most of the problems above arise from the fact that the web has been used as a desktop replacement. This has been the driving force for going beyond web-based management, towards a new management paradigm capable of exploiting web technologies while being integrated into the desktop.

Desktop-based management is the activity to manage networks and systems using standard desktop tools (for instance a text editor), methods (drag and drop) and paradigms (trashcan). The principles behind desktop-based management are:

- Every management resource/information must be accessible from the desktop.
- The composition of management information (for instance weekly router usage) should be accessible from the desktop, hence virtually from every appli-

Poster proceedings of IM ’99, Boston, May 1999.

cation.

- Every management resource should be visible at desktop level (for instance into the filesystem) and accessible from several applications.

The main difference between web and desktop-based management systems is that in the first case network management services and applications are accessible only within the web browser whereas in the latter are available to every application that has access to the desktop. Web-based management can be seen as a special case of desktop-based management where the desktop is restricted to the browser.

In order to demonstrate how desktop-based management works, the author developed *SMB_SNMP*[1] a simple desktop-based SNMP management system. SMB_SNMP is a Samba extension that allows SNMP resources to be managed as normal files and folders from a desktop environment. SMB_SNMP is composed of a MIB compiler called `SNMPTree` and an extended Samba daemon. During the configuration phase, `SNMPTree` reads the available SNMP MIBs and creates a tree of empty files and directories under `/SNMP`, that represent the tree structure as specified by the MIB variable object identifiers. These generated files take almost no space on the filesystem because they are used just as placeholder for representing the MIB hierarchy. At runtime, the Samba daemon intercepts all the calls for files contained inside the `/SNMP` directory and handles them properly. SNMP community values are specified in a configuration file, and security and access control is enforced by Samba itself that prevents unauthorised users from accessing the `/SNMP` directory. Errors encountered during SNMP operations (for instance access denied) are mapped to SMB errors and then presented to the user. Files created by `SNMPTree` have the read/write permissions flags set properly according to the relative MIB, hence errors related to users who attempt to set a read only variable are filtered directly by SMB and do not arise at SMB_SNMP level. SNMP community values are specified in a configuration file, and security and access control is enforced by Samba itself that prevents unauthorised users from accessing the `/SNMP` directory. The `/SNMP` directory can be mounted as a real directory. Variables can be set/read/created both using the command line interface and other applications such as text editors. SNMP tables are represented with a few different files that contain the SNMP table in several formats. Default formats include TEXT, HTML and SYLK in order to allow different applications such as web browsers and spreadsheets to handle table values in a native format without any further conversion. Applications can modify/delete/create SMB_SNMP files. Doing this, the values of the corresponding variables in the agent MIB are transparently handled by SMB_SNMP. SNMP traps can be sent by dropping a file containing the trap value over the special `/SNMP/SNMP_agent_address/sendTraps` directory. Thanks to the Samba flexibility, SMB_SNMP enabled users of popular operating systems to have access to desktop-based management at no cost and without having to install additional software on their client machines.

---

1. The SMB_SNMP package is publicly available under GPL (GNU Public Licence) from the author home page, *http://jake.unipi.it/~deri/*, or can be downloaded from *ftp://sunsite.unc.edu/Linux/system/network/management/*.