

COSduty-SSA V4

A complete system for the management of privileged users

Not only the control of access to confidential online information – as mandated by legislation – but also good security and audit practice can be compromised by granting privileged and often unrestricted access rights (those of the root user or system administrator) to IT operations (production) and administration staff. COSduty-SSA provides the facilities you need to control and audit privileged access without reducing the effectiveness or capability of the people performing the functions for which it is required.

COSduty-SSA additionally allows IT *Operations* best practice and policy to be implemented and imposed, while raising service levels and enforcing both security and auditing. The automation of privileged routines and their delegation to less skilled staff delivers a rapid Return on Investment (RoI).

COSduty-SSA is of great value to organizations with large UNIX and/or Linux infrastructures, with or without a Windows component, who are seeking compliance with Sarbanes-Oxley and other relevant legislation. COSduty-SSA offers a unique combination of privileged user management and IT Operations task scheduling, plus a password vault and automatic, background security checks.

Privileged user management

The key goal of COSduty-SSA is to reduce the use of privileged accounts to the very minimum. One of its facilities is the IT Operations Workflow component discussed later in this document. When access to the 'root' shell, or other privileged account, is required, a request must be made through a COSduty-SSA Access Server for a privileged session. Privileged access is then channeled through a request-approve engine so that administrators

never need to use a privileged user's password.

At the permitted date and time – and, optionally, for a restricted duration – access is opened through the COSduty-SSA Access Server(s) to the particular server ("Managed Server") on which the user requires the privileged session. The session is automatically established using SSH. There is no privileged access to the COSduty-SSA Access Server itself.

Logging of all keystroke activity (including carriage returns) is maintained during the time the administrator is working as a privileged user. All audit trails are retained on a secure Audit Server; tools are available for later analysis of the audit trails to check that no unauthorized activity has taken place.

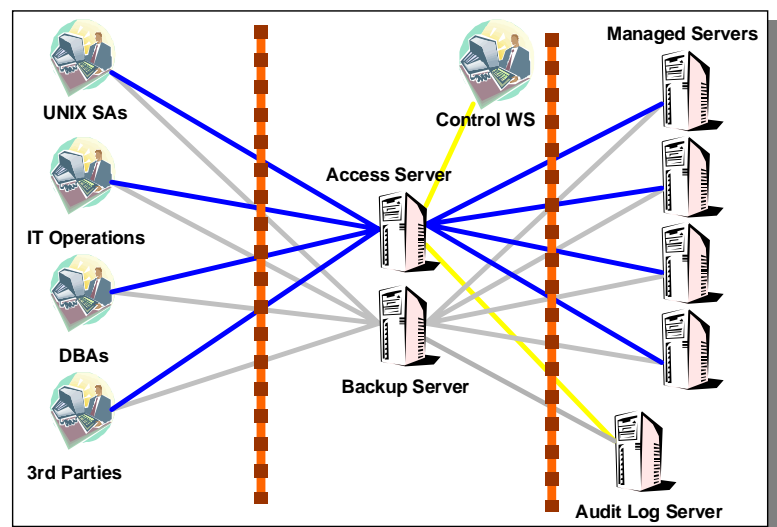


Figure 1 – Secure Shell Auditing (SSA) architecture

Password vault

Under COS*duty*-SSA V4, most system administrators never know the root password, all their activity is audited and system security is therefore very tight. However, there are occasions when engineers and system builders cannot do their work without true local administrator access and must login to the root account. In this case, COS*duty*-SSA's password vault capability is used to manage the use and availability of the root password.

The password vault system enables the generation of new root passwords from the COS*duty*-SSA Access Server at any time. It can be generated automatically in a format according to whatever policy the organization has set (e.g. minimum and maximum lengths, the use of upper or lower case characters, numerics or alphanumeric etc). New passwords can then be automatically distributed to designated groups of Managed Servers; different root passwords can be used for different server groups. Passwords are stored in the password vault in encrypted form and can be recovered only by members of the appropriate role (see below). Privileged user passwords may be renewed regularly and automatically.

The combination of password vaulting for highly privileged access and the normal access controls for everyday administrators significantly improves security, audit and compliance in UNIX and Linux based infrastructures. The combination can also be used to secure privileged sessions in applications including Oracle and the 'administrator' account for MS Windows.

IT Operations workflow

The need to grant privileged user passwords is further reduced by the second major component of COS*duty*-SSA – the Operations Workflow manager.

COS*duty*-SSA enables IT management to enforce best practice and policy across all their computer systems. Instead of having administrators perform the majority of their tasks using a privileged user account (such as 'root' on UNIX or Linux, or 'oracle' on ORACLE databases) with its implied

security, audit and compliance concerns, a facility is provided to store common administration routines and allow their encapsulated form to be executed by means of the Graphical User Interface common to all OSM's products.

Once stored and encapsulated, the routines may be delegated as *duties* to other relatively unskilled personnel to carry out, with benefits in reduced cost, improved service levels, full auditability, improved security, increased accountability and a reduction in dependence on skilled individuals. In particular, routines requiring privileged access by external personnel, e.g. those performing software maintenance or outsourced services, can be executed without their being granted any additional rights.

System administrators can be tasked to record the common routines just once, avoiding the necessity of their having to run them every time. This frees up an organization's most skilled personnel from the mundane, routine housekeeping

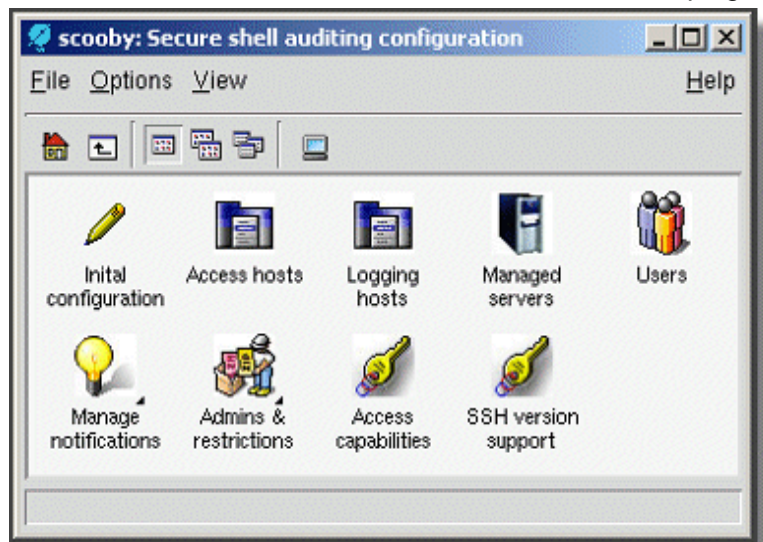


Figure 2 – The OSM Toolset allows technical staff to encapsulate routines in a Graphical User Interface

tasks, allowing them to be more productive and creative, so as to contribute to service improvements

The OSM toolset

An important component of COS*duty*-SSA is the OSM Toolset, a library of software tools that can be used by systems administrators when developing their scripts. Apart from providing a general

productivity gain in scripting, the OSM Toolset allows all resultant scripts to present the user with a consistent and easy to use graphical user interface, and to manage data in a shared underlying data repository using defined communications methods. Cryptic scripts are replaced by easy to use GUI routines that can be initiated centrally but carried out remotely.

The COSduty-SSA operations workflow engine

Once stored and packaged, the routines can then be delegated to individuals or groups of individuals within the enterprise to execute via COSduty-SSA. Instead of logging-in to a shell, staff access these routines, or *duties* as they are now known, via a graphical console display. Duties can be allocated to staff to perform interactively on either an at-request or scheduled basis, or can be run automatically in the background. Users may execute only those procedures assigned to the roles to which they belong and are constrained to operate within the confines of the GUI without the possibility of working in a non-standard way.

In this manner, operations or helpdesk staff members to whom these duties may be delegated are allowed to perform administration routines only as they were stored – so enforcing best practice. All duties are audited as they are performed, and service levels can be checked through appropriate monitoring of the audit trails. Additional service level improvements result from the duties' always being carried out in the same error free manner and by being available to any member of a pre-authorized group so avoiding dependence on any individual.

Duties requiring privileged access can be performed by staff members who will never acquire privileged access for themselves. COSduty-SSA permits safe delegation of privileged procedures to non-privileged staff. The required privilege is assigned to the duty, not to the user. With COSduty-SSA in place, operations staff members no longer require the 'root' password or technical ex-

perience to run standard and repetitive procedures. This enables privileged access to be used only in exceptional conditions.

Through COSduty-SSA, procedures traditionally performed by experienced administrators can now be delegated to helpdesk, operations or clerical end users. Procedures for all systems can be defined on and executed from a central system.

A duty contains the reference to the host or host group it is to be run on. This enables a network of systems to be controlled from a single point. COSduty-SSA ensures that only those procedures appropriate for each Managed Server are made available, and then only to authorized staff.

A duty is run by simply clicking on its entry in the visible list. Views of the console can be chosen to define the duties displayed. The 'At Request' view shows those duties that do not have a schedule.

Duty	Last Done	Who	When	Time
Monthly backup	07/08/04-05:20	COSMOS	Monthly - First Saturday	
Weekly backup	10/08/04-19:00	Bob Murphy	Weekly - Monday	
Move backup media to offsite location	29/07/04-09:45	Ian Stevens	Weekdays	
Search for core files	02/08/04-17:45	Bob Murphy	Weekdays	
Search for large files			Weekdays	
Update anti-virus software on all PCs	26/07/04-10:04	Marked done by Richardp	Weekly - Monday	
Assign Workstation to new employee	06/08/04-14:35	Lynda Hamilton	Once	
Backup CRM database to tape	06/08/04-09:05	Paul Richards	Weekdays	
Check backup logs			Weekdays	
Check for successful database backups	06/08/04-10:19	Bob Murphy	Weekdays	
List all files	05/08/04-06:00	COSMOS	Daily - except Tuesday	
Allocate telephone and ext number	02/08/04-11:34	Paul Richards	Once	
Issue Access Pass	05/08/04-12:53	Stephanie Charles	Once	

Figure 3 – an example of a COSduty-SSA console duty list

The 'Outstanding' view shows those scheduled duties that are now due to be performed.

Once the duty has been successfully run, it can be automatically removed from all operators' duty lists which facilitates the co-ordination of activities amongst a group. When a duty is about to become overdue it is highlighted in a warning color. Staff carrying out a duty are constrained within COSduty-SSA's GUI, and do not normally get any sort of shell access.

Retention of Knowledge

With COSduty-SSA, knowledge (in the form of

procedures) is stored in the database and retained, surviving the departure of key staff from your organization. The same procedures can be performed just as easily by new staff, installed on any new system, or defined and tested at a disaster recovery site.

Such encapsulated knowledge can be specific to a site or generic in its applicability. OSM provides such a generic Knowledge Base (KB) in the form of a set of pre-recorded, background security checks that can be carried out on any UNIX or Linux system. This KB is provided as standard feature within *COSduty*-SSA and adds to the security benefit of the product.

Availability

Sun Solaris, IBM AIX, HP-UX, Linux, Microsoft Windows. Other versions of UNIX and Linux sub-

ject to request.

Summary

COSduty-SSA provides the following benefits:

- simple encapsulation of IT operations' procedures for subsequent execution via a GUI to ensure best practice and policy enforcement
- reduction in dependence on skilled systems administrators
- reduction in operations costs by delegation of complex procedures to less skilled personnel
- reduction in operational errors due to enforced standards
- greater job satisfaction for skilled technicians who are released from routine housekeeping tasks
- service level accountability through auditing of all duties
- improved security through reduction of use of privileged user accounts and password vaulting
- improved auditing as every action generates an audit trail
- greater compliance with legislation that mandates restricted access to data

For more information:

please visit: www.cosduty.com.

The version of **ssa_script** for AIX is based on software developed by the University of California, Berkeley and its contributors



www.cosduty.com

www.osmcorp.com

OPEN SYSTEMS MANAGEMENT, INC.

1511 Third Avenue, Suite 905
Seattle WA 98101
USA

Tel: (866) 601 8011 (toll-free, USA)
Fax: (206) 583 8374
info@osminc.com

OPEN SYSTEMS MANAGEMENT LTD

Kings Ride Court
Kings Ride
Ascot, Berkshire SL5 7JR
UK

Tel: +44 (0)1344 638000
Fax: +44 (0)1344 638011
info@osm.co.uk