



SUN<sup>SM</sup> I-RUNBOOK SERVICE, AUTOMATED EDITION

## A REVIEW OF STANDARD FUNCTIONALITY AND OPTIONAL ENHANCEMENTS

Sun i-Runbook Service

May 2006

## Table of Contents

Abstract.....	3
Introduction.....	4
The case for automation.....	4
Further background.....	5
The Implementation of Sun i-Runbook Automation.....	7
The OSM Toolset.....	7
Delegating procedures.....	8
Monitoring and auditing procedures.....	9
How Users of the Sun i-Runbook, Automated Edition See COSduty-SSA.....	10
Users' experiences.....	10
Optional Extensions to the Sun i-Runbook, Automated Edition.....	11
Privileged user management by controlled access to the "root" account.....	10
Privileged user password secure storage and allocation (the "password vault").....	13
Summary.....	15
Learn More.....	15

## Abstract

The traditional data center runbook is a written set of procedures for both the routine and exceptional operation of systems for use by operators and administrators. The Sun<sup>SM</sup> i-Runbook service is a rational and significant development of the traditional runbook, taking it online using web technology so as to make the appropriate procedures much more accessible and easy to locate. As a web-based online resource, the Sun i-Runbook provides Sun preferred practice procedures that are more robust and link without restriction to other documentation, such as manual pages and additional online resources.

There are sound reasons for the runbook concept to be taken a step further. Having made the major transition from a paper-based to an online resource, the next logical step is for users of the Sun i-Runbook Service to be able to run the documented procedures directly from the on-screen task list with the click of a button. This white paper describes an example of a development that does precisely that. The Sun i-Runbook Service, Automated Edition is the module that, for the first time, provides the framework and user interfaces that allow procedures to be run straight from the Sun i-Runbook browser window.

Although simple in concept, the reality of automating the Sun i-Runbook is quite complex. Not only does the automation system have to reliably manage access control and security, but in the general case and frequently in practice, procedures operate at once on many systems in the data center. Each system has its own peculiarities, such as different administrator user names and passwords, and this knowledge must be embedded in the automation module.

This paper describes the implementation of the Sun i-Runbook Service, Automated Edition by means of a component supplied by Open Systems Management, a Sun Partner. The component is derived from a stand-alone product available under the name *COSduty*-SSA. The product's full functionality is available as an optional addition to the Sun i-Runbook, Automated Edition. The extended functionality, subject to additional licensing, allows data center managers to take further the concept of duty automation, privileged user management and secure password storage.

## Introduction

### The case for automation

The purpose of a runbook, whether paper-based or online, is to provide a source of expertise to the individuals and teams who are responsible for the day-to-day operation and administration of systems in the data center. Today's data center often comprises a large number of networked servers. The the challenge is to be able to manage them collectively from a central point with as few staff members as possible to perform the job reliably.

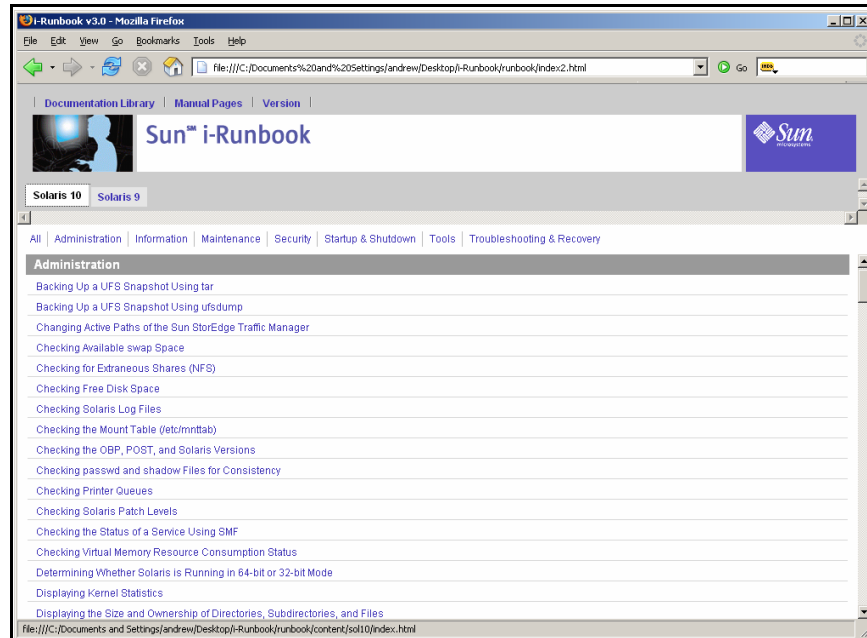


Figure 1—The Sun i-Runbook web-based interface

From time to time, data centers also have to spend heavily on contracted, skilled systems administration staff to assist with the implementation of upgrades and new installations, only to find that the knowledge they bring and acquire leaves when they do.

The advantage of a properly managed and maintained runbook is to encapsulate all such knowledge in a way that is easily accessible to data center staff, with beneficial results such as:

- The encapsulation of procedures help to enable the availability of preferred practice
- Dependence on skilled systems administrators is limited to exceptional circumstances
- Operations costs may be reduced by delegation of complex procedures to less-skilled personnel
- Enforced standards help lead to a reduction in operational errors
- Skilled technicians are used only for exceptional operations and administration duties
- Service levels improve as the result of much improved access to procedures

The runbook and its online version, the Sun i-Runbook Service, deliver major benefits in their own right. However, running procedures directly from the Sun i-Runbook window offers productivity advantages along with less apparent benefits for data center managers. These are especially welcome in today's climate of increased vigilance in the area of access security and the associated area of compliance with legislation and corporate governance.

Additional benefits include:

- Preferred practice is not only immediately available but may be enforced
- Limited involvement of skilled systems administrators may be monitored and audited
- Operational efficiency may be further increased by helping to reduce the running of procedures to a single click
- Operational errors are practically eliminated because procedures are pre-programmed and tested
- Skilled technicians are free to develop new procedures
- Service levels may be calculated and reported from the data collected by procedure monitoring
- Strict role-based access controls on operators and privileged users leads to much improved and demonstrable security

## Further background

In addition to the day-to-day requirements of running an enterprise data center, update or conversion projects can place a significant strain on existing systems administration and operations resources. It is common in such situations to contract for temporary, additional staff whose special skills are required to assist with the project. The problem arises, however, when the contract staff are due to leave. Their special skills in the technical and esoteric areas of implementation often depart with them, particularly because the prolonged use of such experts is costly and cost pressures necessitate removing them in the shortest possible time. The issue is therefore about how to capture and retain preferred practice for future use to help keep the cost of operations to a minimum.

Legislation in the area of corporate governance also has major implications in the area of operations management. The requirement to ensure preferred practice is strengthened by the need to comply with current and forthcoming legislation, which specifies criminal and civil penalties against the officers of companies who fail to take adequate action to protect the integrity of certain types of information.

In the United States, such legislation includes the Sarbanes-Oxley Act of 2002, the Gramm-Leach Bliley Act (GLBA) of 1999, the Health Insurance Privacy and Accountability Act (HIPAA), and the California Database Security Breach Information Act (SB 1386). In Europe, legislation such as the Data Protection Act, Basel II, Higgs, and the Companies Act 2004 is equal to—if not more comprehensive—than that seen in the United States. Senior directors of companies now have to certify the integrity of their financial records. The risk of unauthorized access to systems must be managed, not just to protect the assets and information of the business, but to keep corporate officers free from prosecution.

What makes the problem worse for data centers that have UNIX® and Linux systems is that the majority of those systems are managed by administrators working not through a protected menu system but at the command line (the UNIX "shell"). During conversion projects and for day-to-day management, those administrators have to acquire access privileges greater than those of an ordinary user. UNIX and Linux systems do not provide multiple levels of access privilege, so administrators are obligated to operate at the unrestricted level of super-user.

Unfortunately the command line syntax is not user friendly. The documented procedures of the Sun i-Runbook are a big help to operations staff who are not familiar with the shell's commands but, in order to run them, it is often necessary to first log in as "root" or another user with the same privileges and access rights. At this point, minor errors can give rise to serious consequences, none of which are monitored. Further, the use of the "root" account provides the operator with the ability to access and change any data, including audit trails set up to log their, or any other users', actions. Integrity of data can no longer be guaranteed and the implications go all the way up to the company's financial officers.

This white paper provides details on the implementation of Sun's Sun i-Runbook, Automated Edition. It shows how the Automated edition is not only a simple automation platform for Sun i-Runbook procedures, but also how the implementation brings significant levels of security, role-based access control, monitoring, auditing and reporting, all of which allow data center managers to be confident in the integrity of the data on their systems.

**Adding a Host to the /etc/hosts File**

This procedure describes how to add a host to the `/etc/hosts` file. Information pertaining to the names and associated IP numbers is stored in the `/etc/hosts` file and is manipulated via an editor. The format of this file is two or more columns. The first column is the IP address, the second column is the name of the machine. Third and subsequent columns are aliases by which the machine can be referenced.

**Prerequisites:**

- Superuser privileges are required.
- Must be competent in the use of at least one editor, for example `vi`, `ed`, or a GUI based editor.
- Information about the IP number/host name must be unique.

**Notes:**

- Ensure that the contents of `/etc/hosts` are replicated to each appropriate machine.

Step	Run Task
1	Using your preferred editor, edit the <code>/etc/hosts</code> file and make the appropriate changes.  # <code>/etc/hosts</code>
2	Assuming your network allows <code>ping</code> requests, test access to the specified host by pinging its address. It should respond as 'alive'. If your network disallows <code>ping</code> , use <code>ssh</code> or another method to verify the address.  <input type="button" value="Ping IP"/>  # <code>ping IPaddress</code>  # <code>ping 129.156.93.129</code> 129.156.93.129 is alive
3	Assuming your network allows <code>ping</code> requests, test access to the specified host by pinging its name. It should respond as 'alive'. If your network disallows <code>ping</code> , use <code>ssh</code> or another method to verify it.  <input type="button" value="Ping Name"/>  # <code>ping hostname</code>  # <code>ping prod-13</code> prod-13 is alive

Figure 2—Example Sun i-Runbook Service, Automated Edition procedure with run buttons for both a complete task and running single steps

## The Implementation of Sun i-Runbook Automation

The standard Sun i-Runbook product provides easy and rapid access to procedures for operating and administering systems, at which point the operator must:

- Connect to the system(s) where he/she wishes to perform the procedure, and
- Manually enter the commands that comprise the procedure in a terminal emulation window where a UNIX or Linux shell (command line interpreter) is running.

This has a number of shortcomings:

- The commands entered and run are subject to the standard UNIX access and execution rights, so the operator still may require access as a privileged user (commonly "root"). The operator either has to log in as a user with super-user privileges or, having already logged in under their usual user name, use the 'su' command (with an appropriate password) to achieve the same end,
- IT staff can still make errors during the entering of a command, and
- More than a little familiarity with UNIX system administrator basics is required.

While the Sun i-Runbook Service provides excellent information, it does not help with

- Securing privileged administrator accounts,
- Tracking who is doing what, where, and when, and
- Capturing and abbreviating frequently-used system administrator tasks, such as resetting a forgotten password.

Problems may subsequently arise because the operator, having acquired management privileges, may now go on to do anything on the system that the elevated rights permit, while not at any time being monitored or controlled in any way.

A solution to this problem is to insert a software layer logically above the UNIX shell that can provide the desired functionality. This layer is an essential part of the Sun i-Runbook Service, Automated Edition and is based on *COSduty-SSA*. The technology foundation of *COSduty-SSA* is a structured collection of reusable tools and utilities known as the OSM Toolset.

### The OSM Toolset

The OSM Toolset comprises a number of graphical user interface tools including a forms generator, a browser, a menu tool and several others tools for displaying and managing data. There is also a self-managing, operationally relational database engineered over flat files that allows system files to be incorporated within it, and virtual database tables to be referenced from many commands.

Also contained in the OSM Toolset are several communication utilities, including those with integrated encryption, which can be used or supplemented by others, particularly in the case where the data center wishes to follow its own standards, for example a particular brand of SSH.

The OSM Toolset allows systems programmers to quickly capture procedures for subsequent delegation, with the intention of freeing their own time for more challenging and productive purposes while implementing preferred practice in a controlled manner. Instead of writing and maintaining complex shell scripts in the traditional style, they use the OSM Toolset function library to produce procedures with a graphical user interface that are executable from menus.

Procedures all share the same user interface and become simple to run. It hides complexity. Routines once performed by technical staff become simple enough to be run by individuals without high-level skills, such as help desk, operations, or call center staff.

The staff who run procedures can be confined within the bounds of the OSM Toolset. As well as keeping things simple, the OSM Toolset layer also confines users to the commands offered by its menus, which are themselves sensitive to users' access rights. Procedures are therefore run only by the individuals who are permitted to do so, they always behave as intended by their designers, and preferred practice is thereby enforced.

## Delegating procedures

Procedures, having been captured, simplified, and protected may be allocated or delegated to designated individuals or groups to be run. This process is managed by the *COSduty*-SSA operations workflow engine.

Each procedure is typically delegated to a group of individuals all of whose members possess a particular "role". Allocating procedures to a single individual may mean that those procedures are not performed in their absence and should be avoided.

Once delegated, the procedure is called a "duty". Every duty can be delegated to be run on a scheduled, automatic or "at request" basis. *Scheduled* duties are those that need to be performed on a regular basis, according to a calendar. *At request* duties may be performed at any time by those members of staff authorized to run them, namely those who are members of the appropriate role. Duties that require no interaction are run in the background by *COSduty*-SSA, which acts as a simple job scheduler. Duties requiring interaction with staff may be delegated on a scheduled or "at request" basis.

Duties may be given a meaningful or descriptive name that identifies their function and allows them to be easily selected from a list. In the as-delivered Sun i-Runbook Service, Automated Edition implementation, however, duty names are not presented to operators. The execution of a duty is initiated simply by clicking a button labeled "run task" or "run step," which is positioned next to the description of the procedure that needs to be run. Duty names are much more important to technical staff, whose job is to modify and/or supplement the procedures that come as part of the standard Sun product, using a facility that is available as an optional extension.

Of great importance is the fact that duties (and hence Sun i-Runbook procedures) can be run on any host on the network provided there are *COSduty*-SSA components installed on it. The duty may be performed as any user, for example "root," but without the need for the person running it to ever have access to a shell. In this way the operator never requires or acquires super-user privileges, even if the duty does. The demand for super-user access is reduced and can be kept to manageable amounts.

Users who are members of a *COSduty*-SSA role have access to its duties through the *COSduty*-SSA user interface. Unlike operations staff in a typical UNIX environment, they rarely access a shell, let alone a root shell. Rather, they work from within the GUI as illustrated. No shell escape is available unless it has been specifically allowed, and if it is, the execution of the escape option is monitored along with all other functions within *COSduty*-SSA.

Duties are presented in a context sensitive manner so that individual staff members see only those that they are allowed to perform. Members of the same role all see the same duties and are able to perform them. After a duty has been started by a member of the team, a locking mechanism prevents it from being accessed by the others.

In summary, the use of the *COSduty*-SSA user interface mechanism provides the following benefits:

- Routines that previously would have been carried out by technicians, such as systems administrators, database administrators, and application administrators, can be captured and presented using a common menu and forms structure. The expertise is retained after its author's departure
- Differences between the operating systems of the many hosts being managed, the Solaris™ Operating System (OS) and Linux for example, are hidden by the user interface so that performing the same task on any system or group of systems appears the same
- Policy is enforced and preferred practice can be maintained in a controlled manner
- Errors are virtually eliminated because technical knowledge is captured in programmed procedures rather than being carried out command-by-command in a shell window
- Service levels are improved because more individual staff members can run procedures that were previously dependent on more skilled individuals
- Costs are reduced through automation and delegation
- Accountability and security are improved through the monitoring of all tasks a reduction in privileged access requirements
- Skilled technicians are released from mundane, routine housekeeping tasks and are free to do more productive and rewarding work.

## Monitoring and auditing procedures

While complex and potentially open-ended procedures may be securely packaged for simple execution by means of a single mouse click, there is no guarantee that they *will* be run when the appropriate occasion arises. Some form of recording and accounting is necessary so that managers are able to check that what was intended was, indeed, performed. *COSduty*-SSA, and therefore the Sun i-Runbook Service, Automated Edition, has standard monitoring and audit facilities for this purpose.

A record of every duty is kept with the date and time it was performed, the user who performed it, and under which user name they logged-in before they performed it. This means that in addition to knowing that user "root" performed the duty, managers can see *who* was using the "root" user name at that time. The system(s) involved are recorded, as is the duty itself, along with its exit status and any comments made by the operator. For example, selective reporting of only those jobs that resulted in an error can be extracted.

In this way all staff becomes accountable and their activities and subject to later review. *COSduty*-SSA may even be used as a prompt and confirmation of manual tasks to make sure that there is a record of staff having performed the task in question.

## How Users of the Sun i-Runbook Service, Automated Edition See COSduty-SSA

The implementation of the Sun i-Runbook, Automated Edition was completed with the intention that its appearance and behavior (“look and feel”) are indistinguishable from the other Sun i-Runbook modules. As a result, regular users don't see the OSM Toolset or the other COSduty-SSA components.

Users see the same format of screen layout as for the other modules, with the addition of buttons that are clearly labelled to indicate their function to run a procedure or a step within one. When a procedure or step is run, it is likely that some form of on-screen output is produced that is directed back into the Sun i-Runbook browser window, where it is neatly inserted beneath the display of the procedure's text. At no time is it necessary for an operator to work outside of the Sun i-Runbook browser window. Even the forms containing input fields that request information to be entered by operators while running certain procedures are presented as an integrated part of the Automated Edition's browser display.

Everyday users of the Automated Edition do not need to be concerned with the technology that manages the complex processes running behind the scenes. Users can be confident, however, that a robust, capable, well developed and evolving product helps improve the integrity and reliability of their administration system.

Different considerations apply to skilled technicians and software engineers who may be tasked with customizing their Sun i-Runbook installation by adding local, additional functionality. This is possible if their data center has purchased an upgraded license that gives them access to the COSduty-SSA duty manager, allowing them to write their own duties, add them to the database, and display them as Sun i-Runbook procedures. In this case, duty designers use the COSduty-SSA development environment, which has a user interface constructed with the OSM Toolset.

The as-delivered Sun i-Runbook, Automated Edition is designed so that users are not required to work outside the product's browser window. However, it is possible that local customizations might require special tasks to be performed on systems that require another window to be opened to run them. In that event, activities performed in the separate window should be presented as duties with a user interface and interaction mechanisms managed by COSduty-SSA, using the OSM Toolset.

### User Experiences

Although the Sun Sun i-Runbook, Automated Edition is a new product extension, both its main components—the Sun i-Runbook, Enterprise Edition and COSduty-SSA—can demonstrate significant in-service experience. The following is an extract from a COSduty-SSA case study.

Northumbrian Water Limited (NWL)—the largest independent water company in the UK with very nearly 2m billed customers—operates a data center comprising large- and medium-scale UNIX servers. Constructed on the Oracle RDBMS, the company's main applications are customer billing (ICIS), Oracle Financials, asset management and data warehousing. The company has a major investment in GIS systems.

As well as in the data center, NWL use COSduty-SSA to delegate complex, operational routines to their users within the business. Management at NWL is resolute about defining the policies and procedures that need to be carried out for effective systems management and, in COSduty-SSA, they have a perfect vehicle for rolling them out to operations and business users in a controlled manner.

NWL currently has about 300 captured duties managed by *COSduty*-SSA. Each duty is a complex procedure packaged behind a simple menu/form front-end that allows individuals with modest technical expertise to carry them out in a controlled manner. As an example, even the cashier department in each subsidiary now selects its own reports for printing from available lists, transfers remittance files from mainframe systems to the UNIX data center and moves financial information around the network—all with little knowledge of the underlying infrastructure or operating systems.

"By devolving routines to the originating user departments, we give them a faster service while removing workload from the data center management team," said Malcolm Beckwith, IT data center Manager, Northumbrian Water.

The simplicity of the *COSduty*-SSA user interface is particularly useful. Temporary staff have occasionally to be employed to perform routine work. They can be made productive within hours, and everything they do is monitored and recorded in case their activity has to be reviewed at a later time.

## Optional Extensions to the Sun i-Runbook, Automated Edition

As a consequence of the Sun i-Runbook, Automated Edition's having been implemented by means of OSM's *COSduty*-SSA product, it is possible to extend its standard functionality by writing and adding more duties, which are presented as procedures in the Sun i-Runbook list (described above), and by helping to enable one or more of *COSduty*-SSA's other components, having purchased the relevant license upgrades to do so. The additional functionality is organized into two modules:

- 1) Privileged user management by controlled access to the "root" account
- 2) Privileged user password secure storage and allocation (the "password vault")

### Privileged user management by controlled access to the "root" account

*COSduty*-SSA allows organizations to restrict the use of "root", administrator or super-user privileges by encapsulating privileged commands within a duty. The duty itself may therefore require privileged access rights, but that is acceptable and quite different from an operator's need to acquire personal privileged operating system rights in order to run particular commands.

Many organizations, often driven by audit or legislative requirements, are keen to control privileged access even further because there may be occasions when an administrator requires privileged access even when *COSduty*-SSA is used. While it is not possible to pre-program procedures to cover all situations that may occur, the key is to grant privileged access no more than required and monitor its use in detail. This may become a requirement under legislation as access controls are implemented.

*COSduty*-SSA may be configured to allow authorized users access to either a user shell or a privileged shell. In addition, there is a facility that supports a higher level of control, providing a mechanism that requires staff to make a formal request through the product in anticipation of requiring privileged access. Such requests have to specify time and duration for the privileged user session, and the particular systems on which access is required. Requests are then queued until authorized by whomever is appointed to the task. This facility gives data center managers the option of delegating approval responsibilities to particular, named individuals rather than an anonymous systems administrator.

If the request is approved, a privileged shell is made available for the administrator at the appropriate time on the appropriate system(s). All such access to the managed servers is through the *COSduty*-SSA Access Server, on which root privilege is never granted. During the session all key-strokes are audited, and the audit trails are kept on a separate, secure audit server. Pattern matching searches can later be run against the audit trails to find sensitive combinations of commands, or perhaps for repeated sequences that could better be captured in a duty to remove the need to grant privileged access in the future.

Communication from the *COSduty*-SSA Access Server to the managed server is via SSH, and an agent is installed on each managed server running UNIX or Linux software.

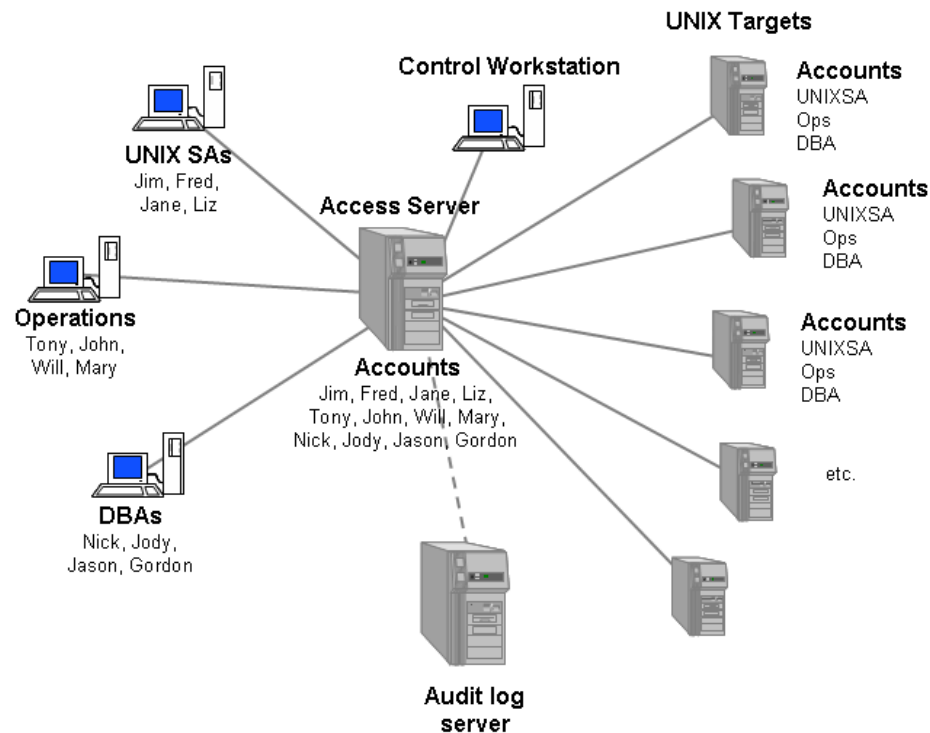


Figure 3 – data paths of the Secure Shell Auditing (SSA) facility

In contrast, the management of privileged access to Microsoft Windows systems utilizes agentless technology. Requests for privileged access ("administrator") are made and approved in the same way. Instead of a session being set up with a remote agent, however, a remote login session hosted by the *COSduty*-SSA Access Server is initiated using the RDP protocol. In this way, access can be granted to a remote user's desktop, or just to a particular application, without the need to install software on any Windows servers or workstations.

At no time in this "request-approval" operation is the root (or other) password provided to the administrator gaining the session. Instead, the session is opened on his/her behalf by a process running on the access server.

## **Privileged user password secure storage and allocation (the "password vault")**

UNIX and Linux are designed so that each system requires a root password to be entered to help enable system administration in single-user or similar management mode. The existence of an infrequently changed root password opens up those systems to abuse from those with sufficient knowledge to take advantage of the fact.

*COSduty*-SSA therefore also includes an optional password vault. In this module, the root password is changed automatically according to a schedule (typically at the end of each working day) and then propagated to all or a relevant subset of remote systems. Different passwords may be used for different groups of managed servers, such as highly secure servers, medium security servers, and less secure servers. The passwords themselves can be generated according to particular rules based on data center policy, such as minimum and maximum lengths, first character to be a number, such as second an upper case alpha.

The new password is stored in an encrypted form on the *COSduty*-SSA Access Server. Only those members of the appropriate *COSduty*-SSA role are authorized to retrieve it. When they do, it can be displayed in clear text for personal transmission to the individual who requires to use it. Between systems, however, passwords are always transmitted in encrypted form if this option is available.

The vaulting service's dependence on the *COSduty*-SSA Access Server necessitates resilient configurations, so either multiple access servers or the *COSduty*-SSA failover software should be deployed.

## Summary

The Sun i-Runbook Service is a relevant and valuable update to a concept that has been in use in data centers for a number of years. Using web-based technology to place the runbook online makes it not only accessible and easy to use, but also enables it to be linked to other documentation and online resources.

Having deployed many instances of the Sun i-Runbook Service, Sun identified a way in which it could be further improved to increase efficiency and address the growing demands for security and accountability. The result is the Sun Sun i-Runbook, Automated Edition, an optional extension to the existing editions and the extensive range of modules.

Although simple in concept, the Automated Edition had to overcome many technical complexities. To bring the new Automated Edition to market in the desired time frame, developers selected an existing software product, *COSduty-SSA*, which is supplied by Open Systems Management, a Sun partner, as the basis for its development.

Relevant features of *COSduty-SSA* are seamlessly used to provide the functionality of the Automated Edition while also solving the technical problems that are inherent to a solution that must span a number of managed systems typically found in today's data center. Automation of the Sun i-Runbook Service brings with it many possibly unexpected benefits, particularly in the area of security and access control, and how such benefits are valuable in meeting the challenges associated with the need for increased security and compliance with recent legislation on corporate governance.

The Sun Sun i-Runbook, Automated Edition may be extended by using additional, optional components from *COSduty-SSA* that add valuable functionality in the areas of privileged user management and secure password storage. Both of these extensions can help a data center improve operational security and demonstrate better compliance with legislation.

## Learn More

For more information about the Sun i-Runbook Service, please contact your Sun Sales Representative or Authorized Reseller or visit <http://www.sun.com/service/irunbook/index.xml>

For more information about *COSduty-SSA*, which was used in the development of the Sun Sun i-Runbook Service, Automated Edition, visit [www.cosduty.com](http://www.cosduty.com)