SAND REPORT

SAND2002-1000
Unlimited Release
Printed April 2000

Final Report for the Account Creation/Deletion Reengineering Task for the Scientific Computing Department

Barbara Jennings and Paula McAllister

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of
Energy under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2002-1000
Unlimited Release
Printed April 2002

Final Report for the Account Creation/Deletion Reengineering Task for the Scientific Computing Department

Barbara Jennings, Project Lead, and Paula McAllister
Scientific Computing Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0807

Abstract

In October 2000, the personnel responsible for administration of the corporate computers managed by the Scientific Computing Department assembled to reengineer the process of creating and deleting users' computer accounts. Using the Carnegie Mellon Software Engineering Institute (SEI) Capability Maturity Model (CMM) for quality improvement process, the team performed the reengineering by way of process modeling, defining and measuring the maturity of the processes, per SEI and CMM practices. The computers residing in the classified environment are bound by security requirements of the Secure Classified Network (SCN) Security Plan. These security requirements delimited the scope of the project, specifically mandating validation of all user accounts on the central corporate computer systems. System administrators, in addition to their assigned responsibilities, were spending valuable hours performing the additional tacit responsibility of tracking user accountability for user-generated data. For example, in cases where the data originator was no longer an employee, the administrators were forced to spend considerable time and effort determining the appropriate management personnel to assume ownership or disposition of the former owner's data files. In order to prevent this sort of problem from occurring and to have a defined procedure in the event of an anomaly, the computer account management procedure was thoroughly reengineered, as detailed in this document. An automated procedure is now in place that is initiated and supplied data by central corporate processes certifying the integrity, timeliness and authentication of account holders and their management. Automated scripts identify when an account is about to expire, to preempt the problem of data becoming "orphaned" without a responsible "owner" on the system. The automated account-management procedure currently operates on and provides a standard process for all of the computers maintained by the Scientific Computing Department.

Acknowledgements

The authors wish to thank the following individuals for their contributions to this project: Sophia Corwell (ReSpec) as Primary Code Developer, Donna Johnson (Compac), James Laros (SNL Scalable Systems Integration), Rosanne Smith (SNL Scientific Computing), Deborah Potter (SNL Customer Support Unit Operations and Development), James C. Hutchins (SNL Information Systems and Development), and Walt Vandevender (SNL Computer Security). The authors also wish to thank John Noe, Manager of Scientific Computing, for enthusiastically supporting this work, Joel Miller (SNL Scientific Computing) for reviewing and editing this report, and the staff of the Scientific Computing Department for their contributions.

Contents

Introduction 7

Background 8

The Goal 9

“Why are we doing what we are doing?” 9

“What steps are necessary? (Are there multiple versions of the same process?)” 10

Proposed Reengineering Process 12

Mobilization 13

Diagnosis 13

Redesign 14

Proposed operations for adding an account: 15

Proposed operations for deleting an account: 16

Implementation 20

Final Outcome 21

Lessons Learned 21

Changes Effected 21

Changes Effected: Corporate 22

Futures 22

References 24

Figures

1. Simplified flowchart of organizations involved in user account addition process 15

2. Simplified flowchart of organizations involved in user account deletion process 17

Tables

1. Corporate resources administered by Scientific Computing 10

2. Old process to create a user account 10

3. Old process to delete a user account 12

4. Revised process to create a user account 16

5. Revised process to delete a user account 18

6. Corporate computers now using the revised process for user account maintenance 20

Intentionally left blank

Introduction

Scientific Computing, Department 9338 at Sandia National Laboratories, is responsible for providing and maintaining corporate computing resources to the Labs' scientific community, on both the classified and unclassified computing networks. At this date, this includes the following production machines[*]: Tesla, Teller, Serber, Edison, Atlantis, Alva, Discovery, sasn100, sasn101, the DEC cluster, the TeraFlop machines Janus and Janus-s, and Cplant, the Linux clustered computer system.

The project to reengineer the process for managing Scientific Computing user accounts followed the methodology of the CMM (Capability Maturity Model) software quality discipline[1] developed by the Software Engineering Institute at Carnegie Mellon University. The intent of the project was to provide an efficient and stable account management process that eliminates duplicative features of existing practices while retaining all requirements and commitments. It was our goal to make the process assure the validity of all user accounts while minimizing operational disruptions and increasing the reliability of access to the systems for our customers: the internal and external users and their projects that depend on the corporate computing resources. Synchronization of our system accounts with the corporate information sources, such as the central NetWork Information System (NWIS), was a primary requirement.

The reengineered product now operates at CMM Level 3. The original account-management process was performed in an ad hoc and oftentimes chaotic manner, because each separate system had its own manual or semi-automated process for account management that was the responsibility of different system administrators to implement. In addition to their regular responsibilities, the system administrators were also spending valuable hours performing the tacit responsibility of tracking user accountability for user-generated data. For example, in cases where the data originator was no longer an employee, the administrators were forced to spend considerable time and effort determining the appropriate management personnel to assume ownership or disposition of the former owner's "orphaned" data files. By reexamining requirements and defining specific objectives we were able to improve the overall process to level 2. The final reengineered product is an automated code written to include the relevant corporate inputs, activities, verification steps and outputs, which meets the standards of CMM Level 3. The software is operational on all of the aforementioned corporate computing resources, and over the course of six months of use has proven to be consistent and reliable. While standardizing the process for adding and retiring computer accounts, the code is updated to accommodate corporately mandated process changes as they occur.

Automation of the computer user account creation/deletion process begins with a data feed initiated by the NWIS. The procedure, in general, operates as follows. Within the Scientific Computing Department there is a computer named Sprocket that serves as the primary source for users' account information. On a nightly basis, a file listing the approved accounts for the machines supported by Scientific Computing is sent by the

[*] The Teller and Serber computer systems were decommissioned in March 2002.

NWIS to Sprocket. An application running on Sprocket processes this file, generating an up to date listing of the account information for each user and providing this information to each supported computer. Sprocket does not have or provide any password information; this information is resident on each specific computer. The Sprocket application determines which accounts are no longer valid and changes the access control files accordingly. Notices are sent out to users with accounts that are within 30 days of impending expiration. The group files are updated with new account information as well.

The reengineered process ensures the integrity of the data required to create and delete user accounts. Thus it ensures the ownership integrity of the accounts for all of the computer systems managed by the Scientific Computing Department. Reengineering the account management process has reduced or eliminated non-value-added work, time, and associated costs in redundant system administration efforts. Most importantly, it ensures that data is managed correctly and within security restrictions on all of the classified and unclassified computer systems supported by Scientific Computing.

Background

The process of adding and deleting user accounts on the computer systems that are administered by Scientific Computing was previously the responsibility of each system's manager. Computer programming scripts to automate the process of adding, but not deleting, these accounts had been written and were operational on the production machines. The general functionality of each of these scripts was the same, to read the NWIS supplied file (Rtflop or Stflop) and add accounts accordingly. However, each script was unique and applicable only to the specific system (or type of system) for which it was written.

Deletion of user accounts was a manual function in order to ensure the probity of each account, that data was managed as required, and that expired accounts were not deleted due to the user's inability to re-open the account (e.g., because of being on extended leave or on travel, or because no notification was received).

It was the desire of the Scientific Computing Department to create a single standardized or "generic" script for the process of adding user accounts, that would run on each system supported by the department. Due to the variety of systems supported, each system's unique "account creation" function had to be implemented in the generic script. Additionally, the process for account deletion was defined (including automatic and manual steps, as required) for each system supported by Scientific Computing.

Each of the original processes for user account creations and deletions were examined step-by-step, identifying the owner and the expected results of each step. A replacement process was then defined using standard reengineering techniques, which:

- lessened the number of procedural steps,
- implemented horizontal integration of required tasks, and

- ensured process integrity among all of the systems supported by Scientific Computing.

The automated process is dependent on the integrity and timeliness of the information received from the NWIS database. In order for the account files to be updated correctly, at least five separate departments within Sandia National Laboratories (NWIS, Password Administration, Scientific Computing, Computer Security Technology, the user's, and the user's department manager or an alternate manager) must take action for each account creation and deletion (deletion might also involve departments in Human Resources and/or Personnel Security). Thus each process was dependent on the performance of, at minimum, six individuals in five departments. Automating the process decreases the bottlenecks inherent in having to rely on specific individuals to complete each task.

The Goal

Reengineering is formally defined[2] as "the fundamental rethinking and radical redesign of the business process to achieve dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service and speed." In practical terms, reengineering means improving a process by reevaluating how it works to add value and by eliminating redundant and/or non-value-added steps. In order to reengineer the existing user account management process two essential questions were asked: 1) "Why are we doing what we are doing?" and 2) "If the current process is comprised of several separate, independently-applied versions, which common steps are necessary and must be retained, which are redundant and can be eliminated, and which steps or ordering of steps can be modified to improve the process?"

"Why are we doing what we are doing?"

It is the responsibility of the Scientific Computing Department to provide vital corporate computing resources to a large number of users throughout and outside of Sandia. In order to be provided this service, a user must have a valid account on each computing system the user needs to access.[3] Maintaining the user accounts on a particular system, including the deletion of terminated accounts, ultimately is the responsibility of that resource's system administrator. On classified networks this responsibility is mandated by the Sandia Classified Network (SCN) Security Plan. Each new user account access request (for account creation or deactivation on any of the corporate computer systems) is initiated by the user (or a user's internal sponsor for an outside account) via a web browser accessing the Web Computer Account Request System (WebCARS) utility on Sandia's unclassified intranet, the SRN (Sandia Restricted Network). For any system on the SCN, account requests require management approval. The information entered into WebCARS is subsequently compiled and provided in electronic file format on the Distributed File System (DFS). System administrators use the DFS files to provide information on the status of accounts on the systems that they are responsible for maintaining. The Scientific Computing administered machines that the user account maintenance processes pertain to are listed in Table 1.

Table 1. Corporate resources administered by Scientific Computing

Machine	Network	Machine	Network
sasn100	SRN	sasn101	SCN
Janus	SRN	Janus-s	SCN
Tesla	SRN	Edison	SCN
Teller[*]	SRN	Serber[*]	SCN
DEC cluster	SRN	Atlantis	SON
Cplant	SRN	Discovery	SON
Alva	SCN		

[*] decommissioned March 2002

“What steps are necessary? (Are there multiple versions of the same process?)”

The series of steps comprising the previous user account creation process, and the individual(s) or group responsible for each step, is listed in Table 2. The process was entirely sequential; each step of the process had to be completed before the next one could be performed. Personnel from five different departments were typically involved in the process.

Table 2. Old process to create a user account

Step	Action	Responsibility
1	User requests account via WebCARS.	User
2	Management approval via electronic signature (WorkFlow group / Jim Hutchins)	Manager
3	Printed approval to Password Administration (PA)	Password Admin.
4	PA validates and initiates account creation	Password Admin.
5	Application creates account updates (John Abbott)	NWIS
6	Account gets moved into tables for update (WebCARS/NWIS)	NWIS
7	File sent to Computer Security Technology	NWIS
8	Active Kerberos created	Comp. Security Tech.
9	Password assigned (Melissa Myerly)	Comp. Security Tech.
10	DCE account created (Melissa Myerly puts in DCE)	Comp. Security Tech.
11	Rtflop/Stflop moved into DFS space nightly (NWIS/Melissa Myerly)	NWIS/ Comp. Security Tech.
12	Scientific Computing scripts read Rtflop/Stflop file via cron utility and initiates script add_user	Scientific Computing
13	New users to Scientific Computing E-mail Administrator (Roy Palmer) from NWIS	NWIS
14	Create new account/home directory	Scientific Computing
15	Link new home directory to DFS	Scientific Computing

The old process for creating user accounts contained four "checkpoints" to validate the process:

1) The user's manager or an alternate manager approved the creation of the account via electronic signature.
2) Password Administration validated the manager's approval (authorization) of the request.
3) A script on the requested machine compared the Rtflop/Stflop file to its current password file to verify new user requests.
4) Roy Palmer, the Scientific Computing Department E-mail List Administrator, verified the new user request against his current mailing lists for each machine and added the new user if necessary.

The process for user account deletion, including the individual(s) or group responsible at each step of the process, is listed in Table 3. Anomalous situations such as personnel being escorted off the premises are not reflected in this table.

The old process for deleting user accounts could involve as many as 7 distinct groups and required at least 19 steps for each request. The steps were all sequential; none of them could be done in parallel. There were three checkpoints to validate the process:

1) The user's manager or an alternate manager approved the account deletion.
2) Dept. 9338 scripts initiated a manual process to verify whether home directories contained files.
3) Roy Palmer compared the request list against the NWIS before removing the names from his mail lists.

There was basically one set of procedures required for completion of user account creation or deletion. However, there were six system administrators, each performing this process on each system that they supported. To answer the second essential question, there were multiple versions of the same process.

The previous processes were not sensitive to the customer and did not always produce reliable data. Due to the sensitivity of classified information, manual intervention is required before system administrators can remove any accounts. There were several checkpoints and yet system administrators found that they had a plethora of issues. Among these were:

- the system administrators were not notified of users who were no longer with Sandia National Laboratories,
- they had a backlog of accounts that were listed for deletion,
- and, there were accounts that were inactivated but could not be deleted (e.g., valid users had not requested re-subscription to an account in a timely manner.)

Table 3. Old process to delete a user account

Step	Action	Responsibility
1(a)	User requests account close via WebCARS for either deactivation or termination of the specific account	User
1(b)	Or, the account expires automatically due to password expiration, regardless of employee status	NWIS
1(c)	Or, Human Resource initiates request for deletion of account via Separation Form	HR
2	Management approval via electronic signature (WorkFlow group / Jim Hutchins)	Manager
3	Printed approval to Password Administration	Password Admin.
4	Password Admin. validates request and initiates account deletion	Password Admin.
5	Application creates table to delete or modify account, updates NWIS (John Abbott)	NWIS
6	Account gets moved into tables for update (WebCARS/NWIS)	NWIS
7	File sent to Computer Security Technology	NWIS
8	New Rtflop/Stflop file created	NWIS
9	Rtflop/Stflop moved into DFS space nightly (NWIS/Melissa Myerly)	NWIS/ Comp. Security Tech.
10	Disable Kerberos accounts and passwords for 5-8 weeks before account is deleted (Melissa Myerly)	Comp. Security Tech.
11	Disable access to DFS (Melissa Myerly)	Comp. Security Tech.
12	SC scripts read this file in a cron and use it to create a list designating user accounts to be disabled	Scientific Computing
13	E-mail updated deletes to Roy Palmer	Scientific Computing
14	Roy Palmer updates mail lists	Scientific Computing
15	Manually edit machine’s password file to remove user	Scientific Computing
16	Manually edit machine’s shadow file to remove user	Scientific Computing
17	Manually edit machine’s group file (/usr/local/system/groups/group_user)	Scientific Computing
18	Former user’s directories are checked for files	Scientific Computing
19(a)	If no files, former user’s home directory is deleted	Scientific Computing
19(b)	Else, former user or manager contacted to transfer files before former user’s home directory is deleted	Scientific Computing

Proposed Reengineering Process

One approach to reengineering[4] [RE] consists of the following phases: Mobilization, Diagnosis, Redesign, and Implementation. A team approach was applied during each of these RE phases as the new process for creating and deleting user accounts replaced the old one, with the purpose of reunifying the tasks into a coherent, reliable, and repeatable process. Members of the team were Barbara Jennings, Sophia Corwell, Donna Johnson, Roy Palmer, Kevin Kelsey, Steve Simonds, Paula McAllister, Geoff McGirt, Eric Engquist, Bill Collins and Doug Pannell.

Mobilization

A RE process must take the perspective of “starting anew,” as if the process has never before been performed. A large portion of the success of RE depends on getting buy-in from the participants who will be affected by the RE. This is abetted by support from the top down as well as by participant commitment. John Noe, Scientific Computing Department Manager, and Jim Laros, Project Leader for the Production Environment, sanctioned this effort, forming a team comprised of system administrators who were responsible for the manual process. Each of the team members, having personal experience with the cumbersome old process, was motivated to have the new process become automated and reliable. Barbara Jennings of the Scientific Computing Department was appointed Project Leader for this activity. Barbara investigated the current operations and socialized the idea of process RE with individuals both within and outside of the department, including those individuals responsible for Sandia’s Business Rules, WebCARS and NWIS. In addition, she sought out the input of Alice Maese, Adaptive Cyber System Deployment & Control Department Manager, on behalf of Pace Vandevender, Chief Information Officer; Craig Jones, Computer Security Site Manager; and R. Michael Cahoon, Computer Security Department Manager, each of whom gave their approval to the idea.

Diagnosis

The pre-reengineering steps for creation and deletion of user accounts are presented in Table 2 on page 10 and Table 3 on page 12. The team determined that the existing account creation process could be automated by utilizing the vendor-supplied “add-user process” for each machine. Once the account data was obtained in file format from NWIS, the remainder of the process to add a user to each system was functional and efficient. The process required corporate data that was synchronized on a nightly basis. Depending on the time taken for approval by the manager, the complete process to add an account could be concluded in 24 hours.

However, the process for deleting user accounts was not as efficient as it could be. Accounts to be deleted were not being verified for file disposition upon user termination or account closure. When a system has files that belong to an account that is no longer active, the system depicts the owner of the file with a numeric identification only (the userID), but without an associated username. Thus the “orphaned” files (those without an “active” owner) became a problem because it was very difficult to determine who the owner(s) of these files should be or was. The importance of computer files to Sandia National Laboratories cannot be determined by anyone other than the owner and (possibly) his or her manager. For this reason, system administrators do not delete any file without the expressed permission of either the file owner or the owner’s manager. Unfortunately, when there is a file without an identified owner, the system administrator of a machine must spend time researching the ownership of the orphaned file. The severity of the problem varies depending on the age of the file and the cause of its abandonment, with the most serious problems arising due to employee termination. Oftentimes, the manager of the user who left files behind was either not the current manager, not familiar with the data, or had terminated as well. At this juncture, the system administrator was in fact performing a task that was certified as having previously been performed according to the employee termination packet.

In reviewing the previous processes, the following points were diagnosed:

1) Sometimes when users' accounts are terminated, files are left behind. Multiple employees in a single department were performing the same tasks to determine appropriate file disposition in order to complete the process of deleting an account.
2) The processes are largely sequential. The steps cross division lines, are "checkpointed" for validation, and require manual intervention.
3) The employment termination process did not provide validation that a terminating employee's data files would be left in a properly accountable state, although the termination paperwork indicated that all computer accounts had been properly closed.
4) Sandia National Laboratories and its customers could be adversely affected by lost data or applications that are not appropriately transferred.
5) Corporate information on account terminations, which was provided as data to Scientific Computing, was not always reliable. Although system administrators could deactivate an account, they did not have the authority to reassign file ownership or to remove the former user's data files and recover the disk storage space without corporate notification of approval.

The team concluded that the old user account management procedures did not meet the needs of the system administrators. The most effective action to take would be to redesign the overall process in order to control or eliminate the three major cost elements that were identified from analysis of the old procedures:

1) The cost that is associated with the system administrators' time being utilized for repetitive administrative processes.
2) The cost to the laboratory and eventually the nation in not being able to perform required computations (in the event of lost or inappropriately deleted data).
3) The cost of employee satisfaction that is affected negatively because system administrators are in the middle of an interdependent process with no control over the steps that must take place.

Redesign

The main goals of the redesign were to delinearize the process to the greatest possible extent, and to improve reliability. In particular, to decrease the number of steps by eliminating redundant and/or non-value-added steps, to reduce the amount of time elapsed between the beginning and end of the process by reducing the sequential dependency of the steps of the process, and to make changes where necessary to ensure the integrity of the data. However, by itself the team from Scientific Computing only had authority to make changes to the final few process steps.

In the old account creation procedure (Table 2, page 10), Scientific Computing was involved in steps 12 through 15. Changes to these steps were recommended. It is the policy of Scientific Computing to maintain an electronic mailing list of valid users (those with approved accounts) for each corporate resource computer. This is primarily for notification capability to keep users abreast of system changes, upgrades, maintenance scheduling, and machine status. The process step for adding users to the mailing list was performed manually, and involved comparing information from two lists (the Rtflop/Stflop file and the existing mailing list). The recommended changes were to make this step become automated, and to incorporate the final two actions within this step.

Proposed operations for adding an account:

Although the procedure would be shortened to 12 total steps, as many as six different groups are involved as shown in the organizational flowchart of the process in Figure 1.

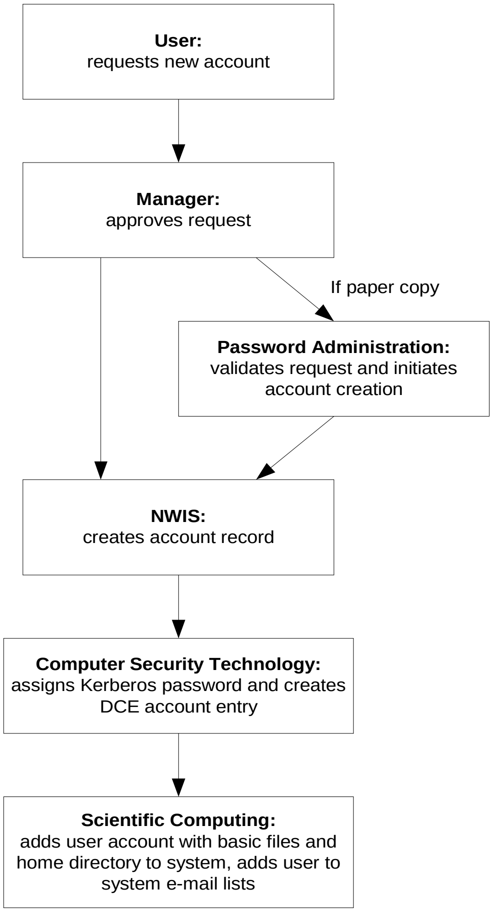
User:
requests new account
Manager:
approves request
If paper copy
Password Administration:
validates request and initiates account creation
NWIS:
creates account record
Computer Security Technology:
assigns Kerberos password and creates DCE account entry
Scientific Computing:
adds user account with basic files and home directory to system, adds user to system e-mail lists

Figure 1. Simplified flowchart of organizations involved in user account addition process

The proposed changes would improve both the amount of time spent during the process and the reliability of the account data. The new account-creation procedure is listed in Table 4, with the revision in bold text. The last four items from Table 2 are now done uniformly, in one condensed step within the departmental process. They are bulleted individually in Table 4 to emphasize to the reader that these are necessary actions.

Table 4. Revised process to create a user account

Step	Action	Responsibility
1	User requests account via WebCARS.	User
2	Management approval via electronic signature (WorkFlow group / Jim Hutchins)	Manager
3	Printed approval to Password Administration	Password Admin.
4	Password Admin. validates and initiates account creation	Password Admin.
5	Application creates account updates (John Abbott)	NWIS
6	Account gets moved into tables for update (WebCARS/NWIS)	NWIS
7	File sent to Computer Security Technology	NWIS
8	Active Kerberos created	Comp. Security Tech.
9	Password assigned (Melissa Myerly)	Comp. Security Tech.
10	DCE account created (Melissa Myerly puts in DCE)	Comp. Security Tech.
11	Rtflop/Stflop moved into DFS space nightly (NWIS/Melissa Myerly)	NWIS
12	**Scientific Computing Dept. scripts read Rtflop/Stflop file via cron utility, which:** • **initiates script add_user,** • **automatically reports new users to Roy Palmer for addition to electronic mailing list,** • **creates new account/home directory,** • **links new home directory to DFS**	**Scientific Computing**

Proposed operations for deleting an account:

The primary driver for RE of the user account deletion process was to improve the reliability of the user-status data received by the Scientific Computing Department from corporate sources. When users terminate their employment at Sandia National Laboratories they are required to fill out a separation form. This form includes a section where the user and his/her manager attest to "Transfer or clear all computer files and passwords." [3] Ideally, this step would require a system administrator for each machine to look at the user's home directory(s) and simply validate that there are no files left with the user as owner. Users are not always performing this directive and managers are not always validating its completion. Consequently, Scientific Computing staff must spend time after the fact doing research to determine data responsibility and more time subsequently to delete or change the ownership attributes of any orphaned files (which in the worst case might be scattered throughout the disk directories). Therefore, this checkpoint was a bottleneck in the process because the process was inherently unreliable.

The RE team proposed a solution to this problem, which would be that the WebCARS development group include a step, as part of the online account request process, to designate an alternative owner for an account. However, the office of the CIO refused this proposal, based on the business procedure that predefines all data as owned by Sandia National Laboratories. Hence the RE team continued the redesign, but limited it to include only those areas that it has direct responsibility over.

There were 19 steps in the original account-deletion process (Table 3, page 12), performed by as many as eight different groups in linear fashion. Figure 2 shows the revised process flow, in which part of the process is now parallel rather than completely sequential.

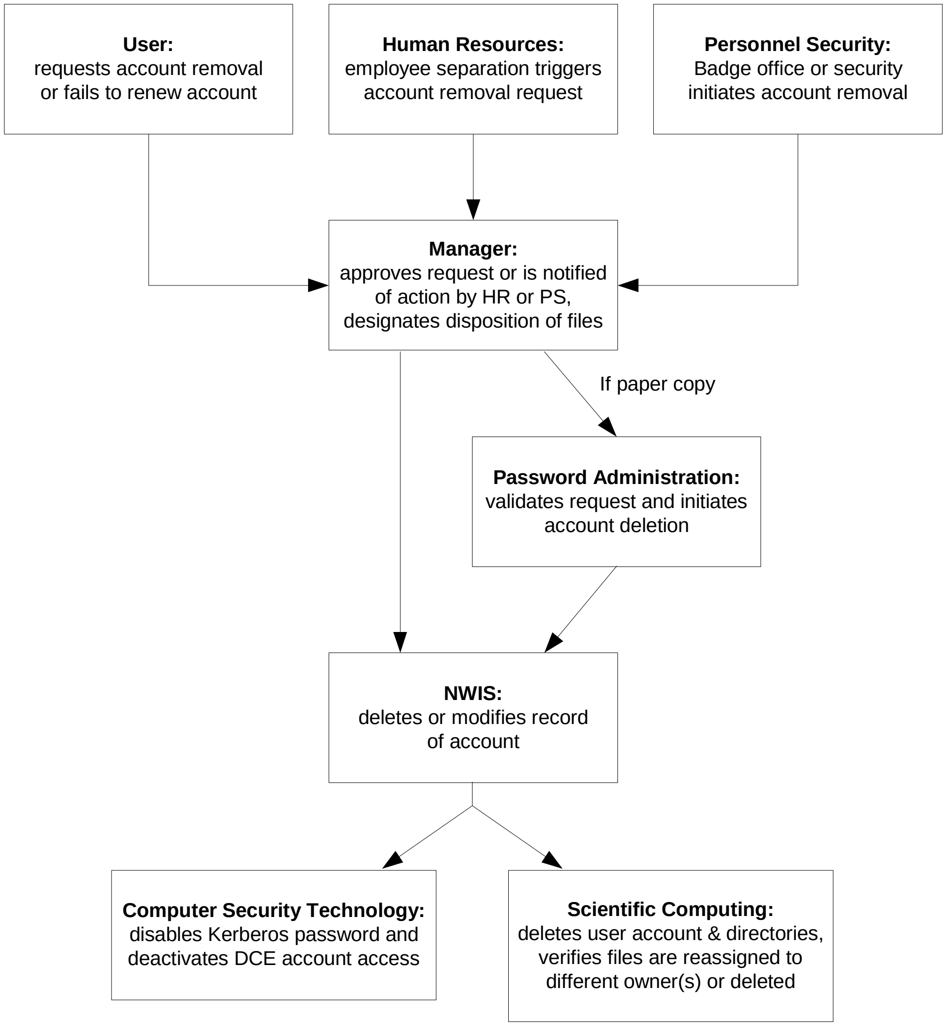
User:
requests account removal or fails to renew account
Human Resources:
employee separation triggers account removal request
Personnel Security:
Badge office or security initiates account removal
Manager:
approves request or is notified of action by HR or PS, designates disposition of files
If paper copy
Password Administration:
validates request and initiates account deletion
NWIS:
deletes or modifies record of account
Computer Security Technology:
disables Kerberos password and deactivates DCE account access
Scientific Computing:
deletes user account & directories, verifies files are reassigned to different owner(s) or deleted

Figure 2. Simplified flowchart of organizations involved in user account deletion process

In order to overcome the problem of file disposition accountability and to improve the reliability of the user-status data received by Scientific Computing, the new process uses a different step order. Scientific Computing is now involved earlier in the process, at step six, the one step in this process that is the full responsibility of the Scientific Computing Department. In order to transfer or delete files, the system administrators will work with the user at this step to guarantee the future accessibility of files for Sandia National Laboratories.

There are 4 occurrences that may lead to the initiation of account closure. These events are defined in Table 5, which identifies the party responsible for the action and the steps that must occur for completion of the request. Changes actually implemented into the new process are indicated in bold; suggested changes are italicized.

Table 5. Revised process to delete a user account

Step	Action	Responsibility
1(a)	User requests account close via WebCARS: *The user is responsible for notifying the system administrator and making the necessary request to perform file disposition, deletion or transfer of files to another authorized user.*	User
1(b)	Or, an account automatically expires (is not renewed): *Notice is sent to the user and the user's manager requesting file disposition. The user or manager must contact password control to reinstate the account or to continue account closure procedures, including file disposition.*	Password Admin.
1(c)	Or, Human Resources initiates deletion of account: *Using information from the Separation Form, the disposition of the user's files is verified.* (Currently, the system administrators are notified of a separation via a standard account closure. However, file disposition designation has not occurred.) *The RE team recommends that a copy of a termination form, which references the specific accounts to be closed, be sent to a designated system administrator for each machine along with certification of file disposition.*	HR
1(d)	Or, Badge Office/Personnel Security Dept. deletion: *The account is removed from NWIS and notification of this action is sent to the employee's manager. The manager must designate file disposition.*	BO/PSD

Step	Action	Responsibility
2	Management approval via electronic signature: *File disposition selection by Manager*	Manager
3	Printed approval to Password Administration; *copy to system administrator*	Password Admin.
4	Application creates table to delete or modify account, updates NWIS (John Abbott)	NWIS
5	Account gets moved into tables for update (WebCARS/NWIS)	NWIS
6	**System administrator** *signs Separation Form, if applicable, and***:** • **verifies file disposition,** • **ensures that user account is deleted from /etc/passwd and /etc/shadow,** • **deletes the user's directories,** • **deletes username entries in /etc/group and usr/local/system/groups/group_users,** • **notifies SC E-mail List Administrator (Roy Palmer) to remove user from e-mail lists** • *returns signed copy of Separation Form to HR*	**Scientific Computing**
7	Updated NWIS file sent to Computer Security	NWIS
8	New Rtflop/Stflop file created	NWIS
9	Rtflop/Stflop moved into DFS space nightly (NWIS/Melissa Myerly)	Comp. Security Tech.
10	Disable Kerberos accounts and passwords for 5-8 weeks before account is deleted (Melissa Myerly)	Comp. Security Tech.
11	Disable access to DFS (Melissa Myerly) This step does not depend on the completion of step 10.	Comp. Security Tech.

The suggested redesign reduces the number of steps from 19 to 11. It is beneficial as it protects Sandia National Laboratories from potential data loss and the cost of time spent at a later date trying to determine the data owner/disposition.

It is important to note that this process is dependent on accounts not being closed via WebCARS until file disposition has been determined and a manager has authorized the closing. The separation form would have to include a signature line for each machine that a user is registered to have an account on.

Employees who initiate account closure would need to verify that all files have been removed from their home/directory(s). Proper advance notice to the user of impending account expiration will negate the impact of abandoned files due to unaware users. Situations involving Badge Office actions (step 1d), such as immediate terminations, will be treated as anomalies and will require the initiators to contact the Scientific Computing System Administrators who in turn would contact the user's manager for file disposition instructions. At this time the Scientic Computing System Administrators feel that they could manage the manual intervention of these anomalies.

Horizontal integration with the Computer Security Technology Department is addressed in this same process. Users would be required to have all files removed from the DFS space. The current process is that Computer Security Technology waits five to eight weeks after receiving an account delete notification before actually deleting the files.

Implementation

The final RE stage was to implement the redesigned process where it was possible to do so (i.e., within the domain of Scientific Computing). This was accomplished via the following steps: gathering specific requirements, redesigning the procedure, and iteratively writing, testing, and rewriting the user account maintenance code. Generic code was written in PERL, allowing it be transportable to all platforms. Different coding adjustments for individual systems were then implemented to match the unique system process requirements. The code was written as five separate modules that run as one process on a central server maintained by Scientific Computing. At the beginning of the implementation stage, the initial module was expected to take approximately six months to write and deploy. Finalization of modules for each platform was expected to take an additional three months. In the end, the effort required a total of twelve months. Lead by Barbara Jennings, the coding work was completed by a team from Scientific Computing. Documentation of the team's efforts was maintained on the department web server sc-admin.sandia.gov. Machines for which the revised user account maintenance process is now (or soon will be) in effect are listed in Table 6.

Table 6. Corporate computers now using the revised process for user account maintenance

Machine	Network	Machine	Network
sasn100	SRN	sasn101	SCN
Janus	SRN	Janus-s	SCN
Tesla	SRN	Edison	SCN
Teller*	SRN	Serber*	SCN
DEC cluster, by machine	SRN	Atlantis	SON
Cplant, by machine	SRN	Discovery	SON
Alva	SCN		

*decommissioned March 2002

Final Outcome

The project to manage user account creation and deletion on the corporate computer systems supported by the Scientific Computing Department was started in October 2000 with completion slated to take nine months. The project completion date ended up being extended three months to October 2001. As of October 2001, most of the machines supported by Scientific Computing on the SRN (Sandia Restricted Network), SCN (Sandia Classified Network) and SON (Sandia Open Network) were operating with the new user account maintenance script. Taking into consideration that this work was performed by individual effort that was above and beyond daily-required responsibilities, the extended time to complete the project was a good investment.

Since its inception, the project endured the following changes:

1) As time went by, fewer team members contributed. As stated, this work was above and beyond individuals' day-to-day responsibilities. Due to unforeseen obligations, not all of those who initially committed to participate were able to. One individual, Sophia Corwell, completed nearly all of the coding for this project. All of the other participants had this task as a lower-level priority due to the demands of system maintenance and customer support. The original number of personnel tasked to code this project was ten. The final number was four.

2) The original project was designed with the intent of being a more general corporate initiative than it turned out to be. Because parts of the process of obtaining and ultimately closing corporate computing accounts are the responsibility of other departments across the laboratory, a proposal to alter the overall process was made, but for various reasons could not be implemented. One of the other departments was making its own change, and others didn't share our view of the need for a change, so in the end we were unable to improve the corporate procedures completely.

Lessons Learned

The Corporate Information Officer's Department defines any file located on Sandia National Laboratories' computers as being owned by Sandia National Laboratories. As such, files are never considered to have been abandoned. Within this constraint, the Scientific Computing Department must ensure the timeliness of accounts in order to track individual responsibility for each computer file, which is established by the computer user identification that is associated with a file when it is created.

Changes Effected

Within the Scientific Computing Department we have instituted a standardized procedure to manage computer accounts on all of the systems that we support. This process is reliable and allows the department to use a common process for all machines rather than having each machine’s system administration possibly being performed in a unique fashion. The user account processes no longer have a single point of administration and therefore are not dependent on a specific individual for completion of user account maintenance tasks.

While each system has unique functions and system requirements, this project provided an improved level of coherency to the systems administered within Scientific Computing. Within a process of consensus, the best process was defined taking advantage of the diversity of talents of the department.

Having a trusted automated user account management procedure in place within the department has relieved individual system administrators of the day-to-day tacit responsibilities for account management. Furthermore, being able to associate each file with an individual allows us to make better use of disk space on our systems. From a security standpoint, we are assured that we are meeting or exceeding the requirements for account integrity on each system supported by this department.

Changes Effected: Corporate

On the corporate level, our suggestions for handling entity accounts were implemented by the NWIS group. Previously, an entity had no human owner associated with it. Today it is treated as an individual account. The account must be approved by management and has an effective date for expiration, and must have approval to be active on a system. The change will negate redundancy of user identification numbers and assign ownership of all of the files and applications on a computer system to identified individuals.

The corporate policy governing file ownership, while not contradictory to the goals of accountability, is too broadly defined to cover the level of granularity necessary for effective system file-management accountability. It is important, however, to know that this policy exists and to learn more about how we can leverage this policy in the future.

Futures

Within the Scientific Computing Department, having experienced the benefits of an automated process for system administration, we have identified and discussed additional procedures that are candidates for automation. These include the gathering of usage statistics that will allow us to provide and analyze metrics.

We plan to automate further the process for deletion of user accounts. This would include the removal of files from user directories in both home and scratch disk areas. The first step is to automate the removal for users who obviously have no critical files (i.e., when the user’s only files are the default files that we provided at account creation). Beyond that, staging files to a temporary “parking” area for ownership reassignment or permission to delete, or checking file disposition and dealing accordingly are possible next steps. Removal will be based on improvements in process, including receiving file disposition instructions from the termination process, if possible.

We also plan to extend this automated process to file ownership within the SMSS (Sandia Mass Storage System). Experience has taught us that archival systems are prone to "garbage in and garbage stays." Ideally, when a storage customer leaves, the customer should go through all storage, removing that which is not useful. Remaining information should be turned over to someone with enough knowledge to use the information. But if there is no one who is knowledgeable, the information loses its meaning. Storing information that is not useful is not in the best interest of Sandia. Our improvements will identify those file elements that are not owned by a current employee.

In addition, automated storage (archival) of historical files related to accounts for each system is desirable.

Other projects that we foresee contributing to operational improvements include:

- standardizing the backup/recovery processes,
- introducing procedures for "productionization" (i.e., bringing a system to production status),
- system maintenance,
- system recovery,
- automation of security log checking, and
- notification of a foreign user on a system (i.e., flagging the GECOS field in the system's password file).

We would like to raise the CMM level of this project to Level 4, Quantitatively Managed, and then to CMM Level 5, Optimization.

We would like to see all computer accounts given higher attention in the procedures for employee separation. It is our belief that the degree to which this can be addressed and integrated into the corporate process will improve its proportionate usefulness for all organizations relying on computer systems, throughout the laboratory.

References

1. Carnegie Mellon University, Software Engineering Institute, Capability Maturity Model, current.

2. Hammer, Michael and Champy, James, “Reengineering the Corporation: a Manifesto for Business Revolution,” 1993.

3. Cahoon, Robert M., “Computer Security Desk Reference,” Computer Security Control No. SNL-DR, Sandia National Laboratories, Albuquerque, NM, current.

4. DeMarco, Tom, “Structured Analysis and System Specification,” 1978.

Distribution:

No.	MS	Org.	
1	0660	9332	Abbott, John P.
1	0807	9338	Amdahl, Robert R.
1	0807	9338	Barnaby, Marty L.
1	0807	9338	Byers, Rupert K.
1	0813	9327	Cahoon, Robert M.
1	0807	9338	Cole, Benjamin H.
1	0807	9338	Collins, William P.
1	0807	9338	Corwell, Sophia E.
1	0807	9338	Davidson, William M.
1	0807	9338	Davis, David D.
1	0807	9338	Davis, Mike E.
1	0807	9338	Engquist, Eric A.
1	0807	9338	Epperson, Marcus R.
1	0801	9300	Hale, Arthur L.
1	0807	9338	Hannah, Michael J.
1	0661	9522	Hutchins, James C.
1	0807	9338	Jaramillo, Frank M.
10	0807	9338	Jennings, Barbara J.
1	0807	9338	Johnson, Donna J.
1	0806	9332	Jones, P. Carol Romero
1	0807	9338	Keeney, Barry E.
1	0807	9338	Kelsey, Kevin M.
1	0807	9338	Kuhns, Victor G.
1	1109	9224	Laros, James H.
1	0622	9323	Maese, Alice
5	0807	9338	McAllister, Paula
1	0807	9338	McGirt, Geoffrey
1	0807	9338	Meyer, Harold E.
1	0807	9338	Miller, Joel D.
1	0363	9323	Morgan, Christine A.
1	0806	9332	Myerly, Melissa M.
1	0807	9338	Noe, John P.
1	0807	9338	Ogden, Jeffrey B.
1	0807	9338	Palmer, Roy
1	0807	9338	Pannell, Douglas
1	0662	9623	Potter, Deborah K.
1	0807	9338	Repik, Jason J.
1	0807	9338	Sanchez, Paul
1	0807	9338	Sault, Allen G.
1	0807	9338	Shirley, David N.
1	0807	9338	Simonds, Stephen
1	0812	9330	Sjulin, Michael R.
1	0807	9338	Smith, Rosanne M.
1	0318	9338	Sturtevant, Judy E.
1	0805	9329	Swartz, William D.
1	0813	9327	Vandevender, Walter H.

No.	MS	Org.	
1	9018	8945-1	Central Technical Files
2	0899	9616	Technical Library
1	0612	9612	Review and Approval Desk, for DOE/OSTI