Hosted Unix (EOS) User's Guide

March 2008

National Institutes of Health
Center for Information Technology
NIH Data Center
Bethesda, Maryland 20892-5607

Publication No. CIT001

Table of Contents

1 INTRODUCTION

1.1 Preface

The *Hosted Unix* (*EOS) User's Guide* provides an overview of the NIH Data Center's Unix-based environment (EOS) for application hosting. We will describe how to establish a new Unix application and how to begin using your application when it is hosted in the NIH Data Center environment. Other information includes operations policies (e.g., security and risk management), charging, systems configuration, and the products and services available to the applications hosted on hosted Unix servers (e.g., Oracle Database Server). CIT communicates important information about the systems via the listserv list used for your specific hosted application (described in Section 2.3.7).

We are here to support you in fulfilling your organization's missions and goals. Please let us know how we can better serve you. If you have comments and questions, please call the NIH Help Desk at:

301-496-4357 (301-496-HELP)
866-319-4357 (toll free)
301-496-8294 (TTY)

or visit **http://ithelpdesk.nih.gov**.

1.2 Overview of Hosted Unix

The Unix-based environment at the NIH Data Center consists of more than 160 servers and currently hosts a variety of production and development applications. The NIH Data Center provides a stable, robust hosting solution for enterprise-wide Unix applications. It features both high-end and mid-tier servers as well as shared and stand-alone servers for Oracle databases and related products, and complete Web capabilities. These hosting services are available on a fee-for-service basis, with the costs charged to your CIT (Center for Information Technology) account.

1.2.1 CIT Services

CIT provides a well-managed server environment suitable for critical Unix-based applications. The NIH Data Center, administered by CIT, acquires and manages hardware and software (e.g., secure-server platform, Oracle licenses). We carefully tailor the configuration to meet the needs of the application.

CIT has long, broad experience in providing production facilities—including 365 days/year operation, physical plant maintenance, system and physical security, disaster recovery procedures, and networking infrastructure. The CIT systems staff is expert in all aspects of operating and maintaining robust, secure system for hosting critical applications.

CIT staff can address your individual computing requirements and help tailor your applications to run efficiently in this environment. For more information, please contact the hosted Unix team through the NIH Help Desk. See Section 1.1.

1.2.2 Summary of the Unix Systems

The NIH Data Center's Unix-based systems provide high performance with an outstanding price/performance ratio. This environment is appropriate for hosting any important Unix-based application and has specific capabilities for applications that use Oracle databases. For more information, see Section 3.

Hardware

Unix database processing is based on HP servers with expandable RAID disk storage. Midrange HP and Sun servers are also part of the Unix configuration and are available for multi-tier or small applications. These midrange servers have proven especially useful for hosting Web servers and middle-tier applications that access secure Oracle databases on the large, shared database servers. Custom configurations are available on Sun and HP hardware.

See also Section 3.2.

Oracle Database Management System

Recent versions of Oracle Database Management System are available on the shared database servers. CIT staff will create and maintain Oracle instances for your application and provide the necessary licenses for direct access to the database. Oracle instance installation, maintenance, monitoring, and procurement are handled by CIT. For additional information, see Section 3.5.2.

Monitoring

CIT staff monitors system availability and resource usage (disk space, memory, and processor usage) on all systems. We provide notifications of system resource issues to our customers 24 x 7.

Connectivity

CIT provides wide bandwidth network connections to and from the Unix systems via SSH (secure shell) protocol, scp (secure copy) protocol, ODBC, SQL*Net, Connect:Direct, as well as via http and https (SSL).

Flexibility

CIT can work with you to develop configurations of hardware and software that match your needs. As your requirements change (perhaps your development system is going production), you can add or subtract additional services and options. You only pay for what you currently use.

Security

Unix is installed, configured, and managed on the hosted systems to provide appropriate protection controls for hosting critical applications and sensitive data for NIH and other government agencies.

The hosted systems are housed in the physically secure and climatically controlled NIH Data Center. Card readers and iris recognition systems restrict access to the facility, temperature and humidity controls maintain an appropriate server environment, and an uninterruptible power supply ensures continuous operations. The systems are monitored 24 hours a day, seven days a week. System data is backed up regularly, and the backup tapes are stored at a remote site. CIT provides an optional disaster recovery program, providing off-site operations at a hot site in the event the systems become in-operational. More information on security is available in Section 2.6.

1.2.3 Proper Use

All users of the CIT enterprise systems, including hosted Unix, are expected to abide by all laws and regulations regarding the proper use of government information technology resources. Users are expected to comply with the following:

- The enterprise systems are to be used for official government business only. Users must not use the systems for personal gain, outside business activities, political activity, fund raising, charitable activity not sponsored by a government agency, or for playing games (even in learning situations).
- Users must not use CIT systems to produce, store, display, or transmit material that is offensive to others including sexually explicit or suggestive materials.
- Users must not use the CIT systems to produce, store, display, or transmit material that constitutes harassment of other individuals on any basis including race, ethnicity, or sexual orientation.
- Users must not use the CIT systems as a staging area for gaining unauthorized access to any other information systems or for, in any way, damaging, altering, or disrupting the operations of the other systems.
- Users must not use the CIT systems and services for capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access to any computer system.
- Access to information on the CIT systems is the sole responsibility of the "owner"—the account sponsor or registered user—of the information. Users must not access that information without the explicit permission of the owner, regardless of the degree of access control applied. The only exception is users may freely access information that is stored under a facility for general availability such as the Web or public libraries.
- Users are expected to use the services and facilities provided by the CIT systems in accordance with the standards set forth in the appropriate guides. If a facility is not described in any guide, contact the NIH Help Desk for assistance before attempting to use it.

- Users must not use electronic communications such as electronic mail to harass others, send obscene messages, forward chain letters or hoaxes, or send mass mailings indiscriminately.

Users who violate these rules of behavior are subject to disciplinary action in accordance with the NIH Information Technology General Rules of Behavior.

Authorities:

- Public Law 93-579, U.S. Code 532(a), the Privacy Act (1974)
- Public Law 99-474, 18 U.S. Code 1030, the Computer Fraud and Abuse Act (1986)
- Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. Part 2635
- HHS Standards of Conduct, 45 C.F.R. Part 73, Subpart M
- NIH Information Technology General Rules of Behavior (can be found at the Web site immediately below)
- CIT Information Technologies Policies Web site at: **http://cit.nih.gov/ITPolicies/**

2 GETTING STARTED

Owners of applications that might benefit from using hosted Unix systems are encouraged to contact CIT to discuss their application requirements. CIT will work with application owners to identify an appropriate hosting architecture – addressing the application's processor, memory, storage, bandwidth, software, and security requirements. The hosting architecture and service/support level that is jointly selected will determine the monthly hosting costs.

2.1 Establishing a New Hosted Application

To request a new application, send e-mail to datacenter@list.nih.gov and provide us with some information about your application. Our staff will then arrange to meet with you to discuss your individual needs in detail.

2.1.1 Acquiring a CIT Account

The customer (application owner) must obtain a CIT account. The charges for using the hosted systems will be billed to this account. Details are online at: **http://support.cit.nih.gov/accounts**. Scroll to the bottom of the page and click on Forms. There is a CIT Account Request Form for NIH Customers and a separate CIT Account Request Form for Non-NIH Customers (an interagency agreement). To initiate a new account, a person with authority to obligate funds must complete the account authorization form for the organization.

Near the end of the fiscal year, CIT sends out a CIT Annual Renewal of Interagency Agreement form to each non-NIH organization using its services. This form must be completed and then faxed or mailed to CIT.

2.1.2 Service Level Agreement

The conditions, responsibilities and costs governing the use of the hosted facilities are mutually agreed to by CIT and the customer through the Service Level Agreement (SLA). After consulting with the customer on the requirements for their application, CIT prepares the Service Level Agreement that outlines the terms and conditions under which CIT will provide hosting services. It lists CIT responsibilities as well as the responsibilities of the customer. The SLA includes a Unix Hosting Service-Level Description document that specifies the facilities, equipment, software, and services that CIT will provide as well as the CIT performance standards.

As part of the SLA, CIT provides a cost sheet for the specified hosting services. The customer must provide contact and billing information. For information on charging, see Section 2.2.

Both the customer and a representative from CIT must sign the Service Level Agreement. Service cannot begin until a signed agreement or amendment is received by CIT. Go to: **http://cit.nih.gov/ProductsAndServices/ApplicationHosting/ApplicationAndWebHosting/UnixSysEOS.htm** for links to a sample SLA and associated documents.

2.1.3 CIT's Role

Once the level of service has been agreed upon and the customer has a CIT account for billing, CIT will arrange for the following:

Application Name

CIT will provide the application owner with the registered name assigned to the application, along with an ID and password for use in accessing the ASR system.

ASR

The CIT Application Service Request (ASR) system allows application owners to request additional application-specific services or to report a problem concerning the hosted application. CIT will authorize you to use the online Application Service Request (ASR) system for your hosted application. ASR provides a mechanism for an owner to establish IDs and passwords for other application members. All account and user management responsibilities related to ASR can be accomplished online. See Section 2.3 for additional information.

Application Listserv List—PROJ List

CIT will set up a listserv list—*application name*-PROJ@list.nih.gov—to be used for e-mailing information on your application to all participants, including the appropriate CIT staff. We refer to this as the "PROJ list" for your application. See Section 2.3.7 for additional information.

Application Coordinators – Your CIT Contact

CIT will assign a hosted systems consultant as your CIT "application coordinator," who will be your primary contact for all matters concerning your hosted application. The application coordinator will be able to help tailor CIT services for your application.

2.1.4 Responsibilities of CIT and the Customer

The Service Level Agreement documents list responsibilities of CIT and the customer. Some highlights are summarized below:

CIT

- provides an application coordinator who will serve as the point of contact with the customer application owner
- gives access to authorized customer staff to the Application Service Request (ASR) system to submit requests or report problems
- provides the physical facility with climate control, sufficient power and backup power, and physical security
- meets with the customer and acquires and configures equipment to meet the customer's requirements

- provides the operating system and supported utility software, installed and configured to the customer's requirements, including upgrades and security patches
- provides system administration including the management of user accounts and timely diagnosis and resolution of hardware and system software problems within the limits of vendor provided assistance
- monitors the systems 24 x 7 and provides system problem diagnosis/resolution
- provides backup services
- provides database management system infrastructure administration, including 24 x 7 monitoring, problem resolution, and security patches, if contracted
- provides middle tier software administration, including 24 x 7 monitoring, backup/recovery/disaster recovery/security implementations, if contracted
- provides perimeter firewalls, network intrusion detection, and host-based security
- provides application firewall services if contracted
- provides secure management in accordance with the Federal Information Security Management Act (FISMA), NIST guidelines, Certification and Accreditation (C & A) security review, and SAS 70 audit review
- provides host-based security solutions installed, maintained, and monitored to prevent system compromises (e.g., virus infections, intrusions, etc.)
- provides disaster recovery services including off-site data storage and hot site availability, if contracted

Customer

- describes all required hours of application availability, and provides management and technical contact information and guidelines for emergency contacts
- if required, coordinates version control of RDBMS and COTS software with CIT to ensure release levels are consistent with operating system levels
- if required, works with CIT to develop a disaster recovery plan and conduct tests
- allowing appropriate lead-time, notifies CIT of functional enhancements that require additional resources
- submits all requests for hosting services, e.g., configuration changes, account administration database changes, etc. through the appropriate communication method (ASR)
- provides contact and billing information
- provides CIT with contact information for problem notification, including off-hours notification and escalation plan
- must respond promptly to any CIT requests to provided directions, information, approvals, or decisions that are reasonably necessary for CIT to perform its services

2.1.5 Application Participants

Your application will have several kinds of participants:

Members include anyone on the application listserv list ("PROJ list")

Authorized Members can submit requests to the ASR system

Application Owners have authority to obligate funds, and can delegate authority to an authorized member; add and remove members from the ASR

2.1.6 Terminating an Application

CIT may terminate any application that compromises the operating environment. If termination becomes necessary, CIT will make every possible effort to work with the application's owner.

If either CIT or the application owner must terminate an application, certain steps should be taken to ensure that the termination occurs in an efficient, orderly manner. Notification of termination by either party should:

- be received by the other party at least 60 days in advance
- be in written form (e.g., e-mail)
- contain the reason for termination

Following the initial notification, the CIT SLA Administrator will send the customer the termination agreement document to sign, along with a final cost sheet for the current fiscal year. CIT staff will work with the customer on arrangements for the disposition of data and associated resources.

2.2 Charging

The fees for the hosted systems can be composed of an initial start up cost, as well as monthly fees for service and storage at the NIH Data Center. If you have questions about systems' charging, please contact your application coordinator. Rates are available at: **http://cit.nih.gov/ProductsAndServices/ApplicationHosting/DataCenterRates.htm**.

2.2.1 Billing

Once a hosted application is established, use of NIH Data Center facilities is charged to the CIT account specified for billing. CIT bills the account monthly for use of the hosted systems.

2.3 Application Service Request (ASR)

Application owners, who need additional application-specific services or want to report a problem concerning the hosted application, must use the online CIT Application Service Request (ASR) system. The primary person responsible for an application is automatically registered to ASR.

Be sure to use the ASR system rather than sending e-mail or phoning staff; these other forms of communication are not tracked and can be lost or incur delays. An ASR notifies the appropriate people (e.g., application owners and CIT staff) about the request and provides tracking and monitoring.

The ASR system provides you with multiple dialog boxes, each containing options appropriate to your application. This ensures that you supply important information before you submit the ASR request.

When you access the ASR system, you will find these basic actions available:

Initiate Request request service for your application

Update Profile update the profile for this user (e.g., change a password)

Manage Request Authorizations authorize other members to use ASR or to be on the PROJ list (if authorized to do this)

Help obtain help about the ASR system

2.3.1 Getting Started With the ASR System

After CIT sets up the ASR system for your hosted application, we will contact you and provide you with your initial registration information.

If you are associated with NIH, you can access the ASR system through your NIH Login. Go to: **http://hosting.cit.nih.gov/asr/nihlogin.cfm** and type in your NIH Login/password. If you are not associated with NIH, or if your NIH badge number is not recorded in your ASR profile, see the topic, "If you do not have an NIH Login" for an alternate login procedure.

To verify that your NIH badge number is in your ASR profile, try logging in to the NIH Login URL above. If your badge number is not in your profile, you will receive an error indicating that you cannot use the NIH Login.

You can add your badge number to your ASR profile by following this procedure:

- Log into ASR using any recent web browser at (case insensitive) **http://hosting.cit.nih.gov/asr**. If you are an Application Owner, CIT will contact you and provide you with your initial registration information—your ASR identifier (i.e., e-mail address). Otherwise, your Application Owner will add you to the ASR system and provide you with this information.
- Click on "Update Profile."
- Add or confirm your NIH badge number.

- Begin accessing ASR using your NIH Login at: **http://hosting.cit.nih.gov/asr/nihlogin.cfm**; you will not need to remember an additional password.

If you forget your NIH Login password, contact the NIH Help Desk. To avoid calling the NIH Help Desk, register for the CIT self-service password management tool, iForgotMyPW (**http://iForgotMyPW.nih.gov**), which allows you to reset your NIH password or unlock your account yourself. You must pre-register for this service.

If you do not have an NIH Login

If you do not have an NIH Login, you can access the ASR system using any recent Web browser at (case insensitive) **http://hosting.cit.nih.gov/asr**. Log in by supplying your ASR identifier (your e-mail address) provided to you by the Application Owner or by CIT.

The first time you login to the ASR system, reset your password by clicking on the "Reset Password" link.

Forgotten ASR Passwords

If you forget your password, click on "Forgot your password?" from the login page. You will have one hour to complete the password change request.

2.3.2 How the ASR System Works

When you enter a request through the ASR system, several things happen:

- CIT opens a Remedy ticket to track the request.
- E-mail containing the request is sent to the project list, which is usually named "applicationname-PROJ." This e-mail list serves as a way to notify its members about information that may affect the application. Appropriate CIT staff are members of the project list along with any application staff members who are registered in the ASR system.
- Further communications about that ASR request are distributed via e-mail to the project list. (E-mail should be sent to applicationname-PROJ@list.nih.gov.) See Section 2.3.7 for additional information on PROJ lists.
- Upon completing the ASR request, CIT closes the Remedy ticket, and e-mail is typically sent to the PROJ list.

Your E-mail Address Is Important

It is not unusual for people to have more than one e-mail address. But ASR recognizes members through a single address. For instance, if you do not access ASR using the NIH Login and you forget your ASR password, you still have to know the e-mail address that is registered to ASR in order to reset your password.

Only project list members are authorized to send e-mail to the project list. So, if you send e-mail to the project list, be sure to send it from the e-mail address that is registered to the ASR system. (You can change your e-mail address by clicking on "Update Profile" in ASR.)

2.3.3 Authorizing Other People to Use the ASR System

If you are the primary person responsible for the application, you are considered the “owner” of the application and as such can manage the membership of the ASR system for your application. An owner can enable additional people to use the ASR system, or can edit or remove the entries for existing members.

To allow additional people to use the system:

- Log in to ASR
- Select “Manage Request Authorizations.”
- At the next page, scroll down and click on “Add New Person.”
- At the “Request to Authorize” page, click the button that allows you to access the CIT Customer Gateway.
- Type in the last and first names of the person to be added in the appropriate boxes. (If the person is not in the CIT Customer Gateway, press the Back button to return to the screen from which you entered the Gateway and press the “Request help/Report problem” link.)
- Follow the online directions.
- You will need to enter an initial password for the person.

You can authorize that person to be on the PROJ list, to submit ASRs, and/or to be a co-owner of the application. Co-owners can authorize other people to use the ASR system or to be co-owners.

Note: CIT will assume that the person making a request via the ASR system has taken into account any cost or system impact associated with the request.

2.3.4 Submitting Application Service Requests

To submit a request for service, go to the ASR Web page and Login. Select Initiate Request. Next:

- Verify your name, phone number, and e-mail address.
- Select the type of service by clicking the appropriate radio button.
- Choose the type of request from the pull-down Service window (e.g., New Unix ID, Recover Unix Files, Security Action)
- If appropriate for the type of service (e.g., Oracle, SQL), select the name of the database instance affected.
- Note: if you are ordering additional equipment (or services) through ASR, the SLA may have to be amended.
- If you want to use a different contact phone number, indicate the desired phone number in the Comments field. If CIT cannot reach you, the request may not be processed.

You must also select the Service Time for the request. The service time choices vary depending on the type of service, but can include the following:

- 2 weeks
- 1 week
- 3 days
- 2 days
- Expedite – Contact within one working day
- Emergency – Page on-call staff

When selecting the time period in the Request Service Time Within window, **please use the Expedite and Emergency service times appropriately**. When an Emergency ASR is entered, the CIT on-call support staff are paged immediately, 24 hours a day, seven days a week. Every effort should be made to plan ahead to avoid emergency situations. Submit emergency requests only in the event of a production work stoppage.

Follow-up

After you have entered your ASR request, the system displays a Service Ticket number. Make a note of that number so you can refer to it if you have questions about the request.

2.3.5 Requesting Security Actions

If you need to request security actions that should be kept confidential and not be visible to all members of the project list, proceed as follows:

- For Type of Service, select Other.
- From the Service pull-down window, select Security Action and hit Continue.
- In the next screen, check the box next to Confidential.
- You must provide a short explanation in the Comments area before hitting the Submit Request button.

Only authorized CIT security personnel will be able to see a Confidential ASR request.

2.3.6 ASR System Help

For additional information on the ASR system, select Help from the ASR login page.

If the ASR system is not usable and a critical emergency occurs, then you should call the NIH Help Desk at 301-496-4357 and explain that there is a critical situation with your application hosted at the NIH Data Center. (The NIH Help Desk can respond to emergency calls 24 hours/day, 7 days/week.) If you call the NIH Help Desk after their normal business hours, you may be prompted for a PIN number. Provide the PIN: 48776 (ITPRO). Please distribute this PIN to any of your staff that you feel may need to handle an emergency situation after hours. Once you enter the PIN, choose from the phone menu for routing your call appropriately.

2.3.7 How the PROJ List Works

Communications about ASR requests are e-mailed to the PROJ list for that application. The e-mail list (*applicationname*-PROJ@list.nih.gov) serves as a way to notify its members about information that may affect the application. For example, if you owned an application called XYZ, you could send e-mail concerning an ASR request related to your application to XYZ-PROJ@list.nih.gov.) The PROJ list is defined so that only list members can send e-mail to the list.

Members in the PROJ list usually include:

- application owners
- other application members registered to the ASR system for your application
- other application staff
- the CIT application coordinator for the application
- CIT staff who participate in setting up and maintaining the hosted application

What Type of Notices Typically Go To the List?

- e-mail from CIT containing an ASR request related to the application
- users' responses to postings
- messages from CIT concerning system changes, maintenance information or potential problems affecting operations
  - at least two weeks notice given for major system changes, patches, or upgrades
  - security patches applied when necessary, with shorter notification periods
- other messages from CIT

2.4 Information for New Users

The following information will be especially useful to new users of the hosted systems.

2.4.1 How to Log In and Log Out Using Secure Shell

Connection to the hosted systems requires use of a secure shell client with SSH2 connectivity, such as SSH Tectia Client (SSH Communications Security). Users must have a static IP address for Unix access or a VPN range of appropriate size.

Important Issues to Remember

- Login with your own individual Unix ID. If you need privileged access, CIT can provide the Unix “sudo” tool.
- Your password will not appear on your terminal when you type it.
- Unix is case sensitive, so you must enter your Unix ID and password exactly correct.
- The first time you log on you must change your password. Reset your password by using the Unix **passwd** command. You will not be able to reuse the same password for at least five generations on most Unix operating systems.
- Changing your password at specific intervals is required. For more information on passwords, see Section 2.6.5.
- **Never leave a session unattended.**
  When you are finished with the session, you can log out by typing the **exit** command.

2.4.2 Getting Online Help

Unix Help

The Unix **man** command gives on-screen information from the Unix “man” pages. These pages contain reference material designed to help you find information about a specific topic. The **man –k** command lets you search for “man” page entries based on a topic or keyword. Given a keyword, **apropos** lists all commands that are related to it. Unix manuals are available from the vendor.

Useful man commands include:

man man	get help about the **man** command
man ksh	get help about the Unix shell program **ksh**

Oracle Help

For help with Oracle products, see Section 3.5.2.

2.4.3 Start Up Files

The default user shell on the hosted Unix systems is **ksh** or the Korn shell. This is the environment provided for interactive users. The “.profile” file in the user’s home directory controls most environment variables. These can be modified to create a customized user environment. Please read the shell man page (**man ksh** or **man profile**) for more information.

2.4.4 E-Mail

When a Unix ID is initially set up on a hosted system, a “.forward” file is created in order to have your e-mail (received locally) forwarded to your preferred mail server. This file should contain a single line with your preferred e-mail address. This e-mail address may be changed to forward local mail to a different e-mail account. **Do not remove the ".forward" file**, as this will make it difficult for you to receive your e-mail.

2.4.5 Editors

The **vi** editor is available for full screen editing over an SSH2 connection. See the respective online "man" pages for more information.

2.4.6 Documentation

In addition to this manual, CIT registered users should refer to *Interface*, a newsletter that contains information concerning services and facilities provided by CIT to NIH and other government agencies, as well as significant changes made to hardware and software on various platforms at the NIH Data Center.

Obtaining Copies

Copies of this manual are available in printed or online format from CIT via the CIT publications Web page at: **http://publications.cit.nih.gov/**. Look under "NIH Data Center Users Guides." *Interface* is available online at: **http://datacenter.cit.nih.gov/interface**.

2.4.7 Training

CIT's Computer Training Program offers database and Unix courses at no charge for CIT registered users. Information on these courses and online registration are available at: **http://training.cit.nih.gov**.

2.5 Operations Policies

This *Hosted Unix* (*EOS) User's Guide* contains information specific to the hosted Unix systems. General information on the NIH Data Center's major systems and development facilities (including database systems) is available from the CIT Web site at: **http://cit.nih.gov**. Select NIH Data Center under Quick Links.

2.5.1 Operating Hours and Availability

Hours

The hosted systems operate 24 hours a day, seven days a week.

Additional information on the operating schedule for NIH Data Center systems is available at: **http://cit.nih.gov/ProductsAndServices/ApplicationHosting/AboutDataCenter/OperatingSchedules.htm.**

Operating System Maintenance

CIT provides the following:

- 24 x 7 operating system monitoring and problem diagnosis/resolution via system experts either on site or on call
- ongoing system administration services (e.g., user account setup, password maintenance, identifying and applying emergency security patches, operation system upgrades, security monitoring)
- minimally disruptive system software maintenance
  CIT can schedule maintenance for non-prime hours. Maintenance is coordinated with the customer except during operational emergencies. CIT sends e-mail through the PROJ lists concerning maintenance that affects their applications.

  Major system upgrades that require longer outages will be coordinated with the customer. Should this occur, notice will be sent at least five business days in advance via the PROJ lists.
- operating system backup and recovery services
  If the system becomes unavailable due to unforeseen events (e.g., power outage), the CIT staff will make every effort to have the system available as soon as possible.
- version control of the operating system, ensuring that the versions in use are fully supported by the vendor
- renewal, maintenance, and upgrades of the system software licenses

Database Maintenance

Database maintenance is coordinated with owners on an individual basis.

Upgrades

For events such as hardware or operating system upgrades, we will work with application contacts to lessen the effect of downtime on applications. Notification includes the date and duration of downtime, the reason for the change, and expected consequences.

Customers requiring CIT to install upgrades should submit the request via ASR. For more information, see Section 2.3 for information on the ASR system.

Major upgrades to hosting facilities are announced through the project e-mail lists.

2.5.2 Backup and Recovery

The NIH Data Center provides backup and recovery services for hosted applications. CIT uses IBM’s TSM (Tivoli Storage Manager) software to perform backups that are then copied to an off-campus location. For information on using the TSM client, see Appendix I. For disaster recovery information, see Section 2.6.

System Backups

At least once a month, system data from production servers are dumped to tape and moved off-campus. The backup tapes stored off-campus can be used to recover the system in the event of an emergency.

Backups of Non-Database Files for Home Directories and Applications

Users' home directories and application directories are backed up through TSM. CIT backs up users' application data according to the customer's agreement. For backups of non-database files, keep the following in mind:

- If there are files and directories in the home directory and application directories that should not be backed up, be sure to inform CIT so that they will be excluded from the nightly backups.
- By default, there are incremental backups performed nightly for all users' non-database directories. These backups are copied to the offsite library.
- Backups for home directories and applications are held for 6 weeks after the file is removed from the system, by default. However, users can request a different retention period.

For Applications Only

- If your application requires different retention criteria or if you want more than two copies of a given file in the backup system, submit an ASR (see Section 2.3.4.) For instance, log files may need different criteria than configuration or data files.
- If you have an application that must be shut down to get a valid backup, we will provide you with a command to run the backup so that you can verify that the application is in an appropriate state.

Backups of CIT-Managed Database Files

CIT performs full physical cold backups of CIT-managed database files each week, using a snapshot technology, where available. Customers can request different retention times and backup intervals.

Backups of CIT-managed database files have the following default characteristics:

- CIT keeps the backups for 4 weeks.
- The first weekly backup of the month is considered a "monthly" backup and is retained within TSM for six months. Monthly backups include both data and executable files.

Backups of Non-CIT-Managed Database Files

If CIT does not manage the database, the customer is responsible for placing the database in a consistent state and creating the backup. Users can write these backups directly to TSM. (Refer to Appendix I.) Or, users can create a backup on a disk that will later be picked up in TSM.

For non-CIT-managed databases:

- The customer is responsible for shutting down or starting up the databases.
- The customer is responsible for verifying the state of the database.
- CIT can provide "sudo" for some commands in order to run commands for creating clones/snapshots in the file system, where available, or for other commands as needed.

Non-Standard Backups

Non-standard backup requests should be submitted using the ASR system. CIT will contact the application owner to work out the details.

2.5.3 Importing Data to the Hosted Unix Systems

Please discuss all data import issues with CIT in advance, so that precautions can be taken to protect the integrity of the system and other users' applications. In many cases, CIT may be able to recommend alternative methods that are compatible with our computing environment.

2.5.4 System Monitoring and Resource Management

What We Monitor

The CIT staff monitors system performance and availability 24 x 7 to verify that the systems are operational and that Oracle databases are available. If problems occur, the automatic monitoring systems notify the staff. Based on the severity of the alert, customers may be notified via the appropriate PROJ list or other expedient means.

Acceptance of Monitoring

The following statement applies to all use of federal IT resources:

> This is a U.S. Government computer system, which may be accessed and used only for authorized Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.
>
> All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system.

Users acknowledge acceptance of these conditions through their continued use of the system.

2.5.5 Increase in Resource Needs

CIT Monitoring of Resources

CIT will proactively monitor application disk space, memory and CPU usage and suggest to the application contacts when it might be appropriate to have their allocated resources adjusted.

When possible, we will increase a customer's disk space when our monitors indicate that the space is filling up. CIT will notify the customer via the PROJ list. If we can't add space dynamically, we will ask the customer to remove some resources or to submit an ASR requesting additional space.

Requesting New Disk Space

Customers can request adjustments to disk space via ASR. If the request is for additional space—and that space is available—the change can be acted on within one week of receipt of the request.

If the storage is in a SAN (storage area network), the request can take up to 2 weeks.

For large amounts of additional storage, please provide at least 60 days advanced notice, when possible, since it may be necessary to acquire and install additional disk drives.

2.5.6 Application Software

If the customer wishes to have software installed on the hosted systems, the application owner should submit a change request via the ASR—see Section 2.3. The application owner should work closely with CIT on such requests. CIT is responsible for ensuring the integrity of the Unix environment, and the CIT staff must first determine the impact of such software on the hosted systems.

If CIT determines that the software is compatible with the environment, CIT will talk with the application contacts about the time required for installation and testing—which varies greatly and is dependent upon both the software and the general circumstances. The application contacts should deliver software and documentation to the CIT application coordinator.

2.6 Security and Risk Management

The NIH Data Center provides a robust and reliable computing environment. This environment includes:

physical access procedures

- controlled access to the NIH campus and the data center complex
- restricted access to the CIT machine room with guards on duty 24 x 7, closed-circuit digital camera monitoring, compartmentalized cardkey access, and iris scans

climate control

- temperature and humidity control for a non-stressed hardware environment *uninterruptible power supply (UPS)*

- designed to provide all electrical services to the machine room area
- fully “conditioned” power with extra-duty battery backup
- diesel generators are available to take over from batteries to provide “never ending” power

24 x 7 system monitoring

- trained staff monitor system status around the clock
- system experts on call at all times

central backup and recovery system

- nightly data backups
- off-campus backup storage

disaster recovery

- regular system-level backups to tapes, which are periodically moved offsite (See Section 2.5.2)
- optional CIT disaster recovery program, if contracted, for continued processing in the event of an extended data center interruption. For more information, visit: **http://cit.nih.gov/ProductsAndServices/ApplicationHosting/DisasterRecovery.htm**.

data and access security

- formal procedures for granting system access
- security violation investigations

firewall services

- NIH network perimeter firewall protection
- firewall services for individual applications, if contracted (see Section 2.6.7 for further information)

system integrity

- intrusion detection
- daily integrity checking

system software is maintained at current levels

- recent vendor upgrades and fixes incorporated into system products and operating system

For questions about security issues, please contact the NIH Data Center Security Coordinator at 301-496-1053.

2.6.1 Security and System Access

CIT requires a static IP address for all users connecting via SSH and scp. Our hosted systems will only accept connections from authorized IP addresses. Submit an ASR to have an IP address added to the access list or to invalidate an existing IP address

2.6.2 System Security

The systems undergo an annual SAS70 security audit. Systems are configured to host critical applications for NIH and other government agencies. When offered by the operating system, the systems are run with enhanced security. All systems' platforms provide enhanced login and password controls, discretionary access controls, user accountability, auditing and account resource limits.

In the interest of system security, the NIH Data Center security officers reserve the right to check user passwords. If a password is "crackable," CIT will notify the user and application contacts to change the password. If the user does not change the password within the designated time period, the account will be locked.

2.6.3 Individual Unix IDs and Role-Based Unix IDs

A unique, individual Unix ID must be obtained for each person requiring direct access to any of the hosted systems. The application owner uses the ASR system to request a Unix ID for an individual. This ID must be restricted to the registered user and should never be shared with others. If there is a need for a role-based Unix ID, which performs a specific function requiring the effort of many individuals, each person should logon to the respective system with their unique ID and then change to the role-based ID using the **su** command.

It is mandatory for the security of an application that this policy be followed. This maintains the user-recognition chain in support of the user accountability requirements of the hosted Unix security environment. In addition, this policy ensures a complete audit trail for each user accessing the system.

If there is any indication that security integrity is being compromised by the actions of a user or application (e.g., by ID sharing), CIT will take immediate action to terminate the suspect activity. Severe or repeated violations of security policy may require removal of an application or user from use of the Unix environment.

2.6.4 Security Data Administration

Historical security data is backed up "forever" for auditing purposes.

2.6.5 Passwords

Passwords form the basis of account usage security. An account that receives more than five consecutive login failures will be locked automatically, on most Unix operating systems.

Resetting Passwords

Reset your Unix server password by using the Unix **passwd** command.

Forgotten Passwords

If your Unix ID has been locked, or if you forget your password, contact your application owner to request that your password be reset. The application owner must use ASR (see Section 2.3) to submit a password change request.

Password Requirements

The various operating systems for the Unix environment have different degrees of password control and restriction. However, all systems have the following minimum requirements:

- All accounts must have passwords.
- Passwords must be changed on initial login.
- ASRs must be submitted to reset forgotten passwords and unlock accounts.
- Passwords **automatically expire after three months**. (This value was previously 6 months; but will be gradually decreased to 3 months for existing accounts.) You will receive a notice at login for 14 days prior to the expiration. You can change the password at any time.
- The password length must be a minimum of 8 characters; this can depend on the individual system.
    - The new password must be sufficiently different from the old one.
    - On Tru64 Unix, HP-UX, and Solaris 10, passwords are not reusable for at least 9 generations.

Tips for Good Passwords

The following tips will make your password more difficult to crack:

- Create a password with a minimum of 8 characters.
- Choose a password with a combination of at least three of the following types of characters:
    - capital letters
    - lower case letters
    - numeric characters
    - special characters (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Change Passwords at least every 90 days to one that is different from your 10 previous passwords.
- Change your newly assigned network password the first time you log on.
- Change vendor-supplied passwords immediately.
- Commit passwords to memory, or store them in a safe place.
- Use only specifically assigned passwords, not those belonging to other users.
- Log out of your computer or lock your screen when you leave your desk.
- Ensure that a password-protected screensaver is enabled on your computer and set to activate if the system if the system is idle for longer than 15-30 minutes. Users have the option to set screensaver activation to less than 15-30 minutes.
- Change password immediately in the event of password compromise.
- Report actual or suspected password compromise immediately.

- If you believe your password may have been compromised, contact the NIH Help Desk at 301-496-4357 immediately.

To create a safe, easy-to-remember password, consider using a short phrase that is meaningful to you and includes punctuation (e.g., “home-again” or “home.again”) or take the first letters and punctuation of a common phrase. For example, the phrase “I love work. I love Fridays” as a password would be **`Ilw.IlF`**. Examples of good passwords are

$L1mERz5 G0ld;karD paS$w3rD

Passwords should be easy to remember but hard to guess. They should not be your ID, social security number, birthday, spouse’s name, or other personal information that is easily obtainable. Never store your password online. If you write it down, keep the written password in a location other than on your computer, preferably in a safe, or other locked enclosure.

For current information on NIH user password requirements, go to:
http://irm.cit.nih.gov/nihsecurity/pwd_requirements.doc.

2.6.6 Unix File Access Controls

The Unix file system defines permissions for the user of a file, members of the group, and everyone else. In a long directory listing (ls -l) the first column should appear something like

```
-rwxr-xr-x
```

This indicates read/write/execute permissions for the user, as well as read/execute for the group and others. To eliminate general access to this file, use the **chmod** command as follows:

```
chmod go-rx filename
```

This will eliminate read/execute commands for the group and others, and the first column will look like

```
-rwx------
```

File permissions are reviewed regularly, specifically for the world write permission bit. If this is set (a "w" in the 3rd set of permissions), then any account on the system can write to the file or directory. This is a major security concern. If you or your application requires the world write permission bit, please provide CIT with a justification. Otherwise, you will receive periodic listings of all world writable files.

2.6.7 Firewall Services for Applications

CIT can provide the following firewall services for an application, with 24 x 7 coverage and support, if contracted:

Security Policy Review and Firewall Policy Development

- review application architecture and application security policy
- assist in the development of an initial ruleset
- represent CIT for customer security audits

Creation of Basic Rules for Administration and Monitoring of the Application

- monitor systems, databases, applications, and networks

Firewall Hardware

- coordinate the redundant firewall system installation
- maintain the firewall system
- work with CIT's Division of Network Systems and Telecommunications (DNST) for infrastructure services

Maintenance of the Firewall Policy Ruleset

- use the ASR system as a secure audit trail in requesting firewall policy modifications
- backup and archive the ruleset
- modify the ruleset in response to changes in the application environment

Troubleshooting

- implement report generation, traffic auditing, and notification of the customer due to any adverse event
- provide expertise in network protocols and architectures to provide an interface to customer network personnel

Collaboration With Application Owners If Their Environment Changes

- analyze changes in policy due to the evolution of the application
- meet with application owners and their security officials to provide a conduit to NIH security officials

For additional information on this service, please contact the hosted Unix team through the NIH Help Desk. See Section 1.1.

3 HOSTED UNIX SYSTEMS CONFIGURATION

The hosted Unix systems are constantly changing, as we upgrade facilities and adopt emerging technologies that will benefit our users. CIT can work with you to develop a special configuration of hardware and software for your needs. As your requirements change (perhaps your development system is going production), you can add or subtract additional services and options.

Changes that affect existing customers will be announced using the appropriate listserv list. See Section 2.3.7.

3.1 Unix Configuration

CIT acquires and configures the hardware and software according to the requirements of the customer and does the following:

- sets up and installs a dedicated Unix server, if required
- provides Unix accounts, group and owner access privileges, and secure TCP-wrapped network connections
- provides an auditable backup and recovery environment

3.2 Hardware

The hardware used by the hosted systems is stored in CIT's highly secure machine room.

3.2.1 Servers

HP Servers

Our systems feature multiple HP servers—ranging in size from midrange to high-performance application servers. Customized configurations are available depending on the requirements of the application.

Sun Servers

CIT provides multiple Sun 2- or 4-processor midrange enterprise servers.

Other configurations are available depending on application requirements.

3.2.2 Storage

Hosted Unix systems provide online storage for data as needed. Storage can be provided on SAN (storage attached networks) or locally attached storage, depending on the system, application, and storage required. Most storage is provided in a RAID configuration for reliability.

3.3 Software Overview

CIT provides the following software for the hosted Unix systems.

Operating Systems

Tru64 Unix
Sun Solaris
HP-UX

Database

Oracle on shared or dedicated Unix servers

Connectivity

FISMA-compliant highly available, secure connectivity, such as:

SSH
Connect:Direct

Middle Tier Application Servers

Oracle Application Server (see Section 3.5.1
Netscape Enterprise Server (see Section 3.4.2)
Apache Server (see Section 3.4.2)

3.3.1 Customer–Supplied Software

If the customer has supplied software for the hosted systems, the customer is responsible for supplying CIT with all updates to software, licenses and documentation. The installation of customer-supplied software should be discussed with CIT staff. See Section 2.5.6 for additional information.

3.4 Major Applications Provided by CIT

This section describes applications that are available on the Unix platform. Before using these or any additional applications, please consult with CIT staff. Generally, the application owner registers users for these applications by submitting an ASR. Refer to Section 2.5.6.

3.4.1 Connect:Direct

Connect:Direct is a product for transferring data—especially financial transactions—between different computer systems. It can be used for transactions with the U. S. Department of the Treasury. Connect:Direct monitors the progress of the file transfer.

CIT will work with the application owner to determine whether Connect:Direct can benefit your application. Connect:Direct should be part of the service negotiated with CIT.

Connect:Direct Secure+

The Connect:Direct Secure+ option provides strong mutual authentication, data encryption, and data integrity checking for Internet transactions. It uses Secure Socket Layer (SSL) technology to encrypt data as it passes between Connect:Direct nodes.

3.4.2 Web Servers

Netscape Enterprise Server (NES) and Apache HTTP Server are powerful Web servers for enterprises with large scale Web sites. These servers also enable rapid development of Web-based applications that can enhance communication, streamline processes and reduce costs. CIT also supports the Oracle Application Server for Web development. See Section 3.5.1.

3.5 Oracle

Oracle products can be installed on both shared and dedicated machines, depending on the requirements of the application.

3.5.1 Oracle Application Server

Oracle Application Server, "middle tier software," allows for developing and deploying applications for the Web. Its scalable, distributed architecture and database integration provide a foundation for supporting enterprise-critical applications accessed from Web browsers. This server is also a strategic platform for network application deployment that brings substantial savings over client/server-based applications through reduced complexity, better manageability, and simplified deployment. The Oracle Application Server instances are installed, upgraded, and maintained by the NIH Data Center. There are a variety of installation options for the Oracle Application Server.

Oracle Application Server should be part of the service negotiated with CIT.

3.5.2 Oracle Database Server

Oracle Database Server is a high-performance database engine capable of handling large amounts of data, images and many concurrent users. It offers backup and recovery facilities and excellent security. The Oracle Database Server instances are installed, upgraded and maintained by the NIH Data Center.

Oracle data is accessible interactively via client/server and Web connectivity or an online connection. It can also be accessed by batch jobs. Online and batch application programming facilities allow programmers to embed SQL statements in C/C++. Client/server access allows an almost unlimited application development environment, including 4GL and Web environments. This capability allows users to create custom-tailored interfaces to Oracle data for their applications and to perform sophisticated data validation as it is entered.

There are a variety of installation options for the Oracle Database Server on the hosted Unix systems.

Oracle User Accounts

The application's database administrator (DBA) must have an Oracle user account. After the installation of an Oracle Database instance, CIT will create an Oracle user account with the privilege of DBA role for the application's DBA use. The application DBA can then create and maintain additional Oracle user accounts within the database instance.

In addition, Oracle application users may desire a Unix ID if they want to store application documents as Unix files or run Unix-level applications or scripts. A Unix ID can be requested via ASR.

Basic Oracle Set Up

The basic service fee for Oracle Database Server instances includes installation and maintenance, upgrades and database systems support, as well as backups of Oracle system software and database files. For information on backups of CIT-managed database files, see Section 2.5.2.

The basic fee also includes two dedicated Oracle instances—one for production and one for development/testing—and full public internet access for the application if desired.

Assistance for Database Users

CIT provides a stable software and data-repository environment for enterprise-wide database and information systems at the NIH Data Center. CIT assists organizations in implementing appropriate technologies to meet their centralized database and information processing needs, and keeps abreast of promising database and information processing technologies. Users can take advantage of the free CIT Computer Training Program (**http://training.cit.nih.gov**).

Support

To report a problem concerning the hosted application, use the CIT Application Service Request (ASR) system. See Section 2.3.

Documentation

Users can view Oracle documentation online from: **http://www.oracle.com** or purchase manuals from the vendor.

Sizing Considerations

The application contacts should work with our staff to determine sizing requirements—including optimal memory utilization, system global area and disk utilization—for their database and application.

Server Options

Replication

Replication is a mechanism for supplying updated information across servers. Basic replication uses “read-only snapshots” to enforce a form of primary site replication. Such a “snapshot” is a full copy (or a subset) of a table that reflects a recent state of the master table. Replication is done to speed local queries and provide a degree of redundancy.

Intermedia

This Oracle option is a text management solution that enables you to manage unstructured text information resources with the same security, scalability, and integrity as structured data that is stored in columns. With this option, you are able to build and deploy text-based applications with an SQL-like interface.

Oracle Advanced Security

Oracle Advanced Security provides transparent data encryption of data stored in the database, the encryption of disk-based backups of the database, and also network encryption for data traveling across the network between the database and client or mid-tier applications. It provides a complete suite of strong authentication services to the Oracle database.

Version and Patch Levels

CIT’s Oracle systems support staff will work with application contacts to coordinate changes to the database version levels and patches.

Appendix I – Basic TSM Information

Basic TSM Information

(Some of the information that follows is adapted from *IBM Tivoli Storage Manager Concepts* by International Technical Support Organization, IBM Corporation and *Tivoli Storage Manager for Unix: Backup-Archive Clients Installation and User's Guide*, Version 5.3, IBM Corporation.)

This document is intended to be a synopsis of useful TSM commands and features and a guide to understanding TSM as used at CIT.

- The **TSM client** holds the critical data that has to be protected. In the case of the hosted Unix systems, the TSM clients are the Unix servers.
- The client's data is sent to the **TSM server** through TCP/IP. The TSM server stores the data in TSM storage pools and uses a database and recovery log to track the location of the data in the storage pools.
- TSM storage is either in the form of a backup or an archive.
    - A **TSM backup** creates a copy of a file in the TSM server repository. Multiple versions of the data object can reside in TSM as the original object is modified. The number of versions of a file that TSM retains is controlled by server definitions. The presence of the original is also related to the presence of the copy in TSM. (See the backup retention parameters below.)
    - A **TSM archive** is a file or collection of files stored in TSM for a specified length of time.
- TSM interaction is available via the TSM GUI (dsm) or the command line (dsmc). Further details of both methods can be found in *Tivoli Storage Manager for Unix: Backup-Archive Clients Installation and User's Guide* referenced at the beginning of Appendix I.

Query

To find out what is backed up, the TSM *query* command is used. Files displayed are owned by the user executing the command.

The *query backup* command displays a list of backup versions of your files. For each backup version, TSM displays the file specification, file size, backup date, whether the file is active or inactive, and the management class to which the file is assigned.

The *query archive* command displays a list of your archived files, the file size, archive date, file specification, expiration date, and archive description.

The query command includes the file specification for which to search and can include options to help narrow the search.

Example:

```
    query backup –fromdate=04/01/2005 /usr/users/james/myfile
    query backup –inactive "/usr/users/james/mydir/*"
```

A full list of options is documented in *Tivoli Storage Manager for Unix: Backup-Archive Clients Installation and User's Guide.* The more useful options that can be used are:

- fromdate -- specifies a date from which you want to search for backed up or archived files. Files that were backed up or archived before this date are not included, although older directories might be included, if necessary, to restore or retrieve the files.
    - –fromdate=01/01/2006
- fromtime -- used with the **fromdate** option, specifies a beginning time. This option is ignored if the **fromdate** option is not specified. Time is HH:MM:SS using a 24-hour clock.
    - –fromtime=16:00:00
- todate -- specifies an ending date. Use the **todate** and **totime** options with the **fromtime** and **fromdate** options to request a list of backed up or archived files within a period of time. For example, you might request a list of files that were backed up before Jan 30, 2006 or those that were backed up between 6:00 AM on Jan 1, 2006 and 11:59 PM on Jan 30, 2006.
    - –todate=01/30/2006
    - –fromdate=01/01/2006 –todate=01/30/2006 –fromtime=11:59:00 –totime=06:00:00
- totime -- used with the **todate** option, specifies an ending time on a specified date. Use the **totime** and **todate** options with the **fromtime** and **fromdate** options to request a list of files that were backed up within a period of time.
- inactive -- used to display active and inactive objects. This will include all versions of the object in the backup system. The **fromdate** and **todate** options can be used to specify a specific version.

Storage Classes and Retention Criteria

- As files are backed up or archived they are associated with a "management class". The management class is defined by the TSM administrator and determines the retention parameters.
- Different directories or even different files, as long as they can be specified via wildcard matching, can have different retention criteria.
- Specific files or file systems can be excluded from the incremental backups if the incremental backup would result in an unusable file. One example of this would be an Oracle database (.dbf) file. Since all files would need to be backed up with the database down, backing up one database file would not be a consistent database backup.
- For queries and restores, TSM differentiates between a file that exists on the client (active versions) and older versions of these files or files that have been removed from the client (inactive versions). The active version is always the most recently backed up version. Archives are a complete collection of files and are not concerned with active/inactive versions.
- Backup parameters set by the management class are:
    - VEREXIST - The number of versions of a file kept in TSM. The oldest version will be removed from the TSM system to make room for newer versions.
    - VERDELETED – The number of versions of a deleted file that should be kept in TSM
    - RETEXTRA – Length of time to keep the extra (inactive) versions
    - RETONLY – The length of time to keep the last version of a file after the file has been deleted.
- The default management class will retain files as follows:
    - VEREXIST=3, VERDELETED =2, RETEXTRA =30, RETONLY=90
    - Up to 3 versions of the file will be available in the TSM system as long as the file remains on disk.

- Once the file has been removed from disk, TSM will retain up to 2 copies.
    - The inactive versions in TSM will remain for 30 days.
    - The last version of a file (inactive) will remain for 90 days.
- Both the parameters for the number of versions and the parameter for the length of time are involved in determining how long inactive versions are kept.
    - If VEREXIST is 3, and there are 3 copies in TSM, the oldest one will be removed from TSM the next time the file is modified.
    - If VEREXIST is 3, RETEXTRA is 30, and there are 3 copies in TSM, if the file is not modified again the oldest version will be removed from TSM when it is 31 days old, leaving 2 versions in TSM.
- Archive parameters set by the management class are:
    - RETVER – length of time the archive should be retained.

Backup

Incremental backups occur nightly. If you change a file and want it backed up immediately, the owner of the file or other authorized user can back up the file or directory with the command

```
     dsmc selective “FILENAME”
```

Be aware that this increases the number of versions of the file in the TSM system, and older versions may therefore be removed from TSM. To request specific retention criteria for a file, group of files or directory, please submit an ASR.

Frequently Used Commands

- To find all versions of files (old copies as well as current) from a directory

```
query backup –inactive /home/james/mydir/
```

- To find all files that had been backed up from the directory /home/james/mydir between 1/1/06 and 1/30/06, even if they have since been deleted from disk

```
dsmc query backup –inactive –fromdate=01/01/2006 –todate=01/30/2006/home/james/mydir/
```

INDEX

Hosted Unix (EOS) User's Guide

Document Evaluation

Is the Manual:

	Yes	**No**
Clear?		
Well Organized?		
Complete?		
Accurate?		
Suitable for the beginner?		
Suitable for the advanced user?		

Comments:

Please give page references where appropriate.

If you wish a reply, include your name and mailing address.

Send to: The NIH Data Center
Center for Information Technology
National Institutes of Health
Building 12A, Room 4011
Bethesda, MD 20892-5607

FAX to: 301-496-6905

ICD:
Date Submitted:
Name (Optional):