

INTERIX™

## Technical Note #0008

v1.2 June 15, 1998

Softway Systems, Incorporated  
185 Berry Street, Suite 5514  
San Francisco,  
California, USA, 94107

(415) 896-0708  
Fax: (415) 896-0709  
<http://www.interix.com/>

# Inetd and the Rutils

INTERIX Developer Support

## Contents

**What is inetd? 4**

**Security and Inetd 4**

    Why a Domain User Account? 6

    The Account Running inetd on Workgroups 7

**Overview: Setting Up Inetd 7**

    Creating the inetd Account 8

    Start inetd as a Service 10

    Start syslogd as a Service 11

**Disabling a Daemon 11**

**Specific Daemon Notes 11**

    ftpd 11

    inetd 11

    ntalkd 12

    rdist, rdistd 12

    rcp, rlogin, in.rlogind, rsh, in.rshd 12

    talk 13

    telnetd 13

    tftpd 13

**Note for Users of rlogin, rsh and rcp 13**

    Testing the .password File 15

## **Technical Note #0008: Inetd and the Daemon Package**

Written by John McMullen and Rodney Ruddock

### **Copyrights**

Copyright © 1998 Softway Systems, Inc. All rights reserved. You may not copy this document in whole or in part without prior written permission from Softway Systems, Inc.

This product includes software developed by the University of California, Berkeley and its contributors.

### **Trademarks**

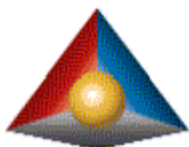
INTERIX and OPENNT are trademarks of Softway Systems, Inc.

Microsoft and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and /or other countries.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated which may be registered in certain jurisdictions.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through The Open Group.

All other products mentioned are trademarks and registered trademarks of their respective companies. Mention in this document is for informational purposes only and there is no intent to infringe upon existing trademarks and properties.



## Inetd and the Rutils

This is a summary of how to use the **inetd** “super server” with INTERIX and the related daemons that can be started with **inetd**. Complete information on each daemon and utility mentioned herein can be found on its reference page (e.g. **man inetd**).

The package contains **inetd**, the “super server” and its configuration file **inetd.conf**; and the following “daemons,” utilities, and files (installed under **\$OPENNT\_ROOT**):

- bin/rcp**
- bin/rdist**
- bin/rdistd**
- bin/regpwd**
- bin/rlogin**
- bin/rsh**
- bin/talk**
- bin/tftp**
- etc/inetd.conf**
- usr/sbin/in.fingerd**
- usr/sbin/in.rlogind**
- usr/sbin/in.ftpd**
- usr/sbin/in.ntalkd**
- usr/sbin/in.rshd**
- usr/sbin/in.telnetd**
- usr/sbin/in.tftpd**
- usr/sbin/in.rexecd**
- usr/sbin/inetd**

Note that most of the daemons are in the subdirectory **usr/sbin**. Users with a Linux or BSD background may be surprised by the daemon names, which conform to the System V convention. Man pages are available under the “root” name (i.e., **man telnetd** instead of **man in.telnetd**).

There are two identical copies of the **telnetd** binary, **bin/telnetd** and **sbin/in.telnetd**. The **in.telnetd** copy is specified in the **inetd.conf** file. The copy in **bin** is maintained for backward compatibility and will eventually disappear. The **regpwd** utility is used to create **.password** files (see “Note for Rcp, Rlogin, and Rsh Users”).

**Note:** For security reasons, this INTERIX port of the FTP server, **in.ftpd**, does *not* support anonymous ftp. For more information about the security of this package, see “Security and Inetd”, below.

If you have difficulties using these daemons and utilities after reading this paper and the appropriate reference pages please contact [inetd@interix.com](mailto:inetd@interix.com).

---

## What is inetd?

**Inetd** is a “super server” that allows your system to serve many internet services such as **telnet**, **rcp**, and **ftp** to many users at the same time, while using minimal system resources. **Inetd** may be thought of as a doorman: when someone knocks at the door **inetd** answers the door and then gets the program that the caller is seeking.

In more technical terms, **inetd** listens for remote connections to TCP / IP sockets with well-known addresses. Each well-known address is associated with a specific service (e.g. **ftp** is associated with port 21, **telnet** with port 23). Once a remote request is detected, **inetd** starts the appropriate service for that well-known port. The freshly-started service then picks up the socket connection(s) and performs all of the protocol / data-exchange specific to that service.

The services that **inetd** can start are specified in the configuration file **\$OPENNT\_ROOT/etc/inetd.conf**. The **inetd.conf** file installed with the “daemon pack” needs no changes unless you wish to “turn off” one of the services. (See “Disabling a Daemon,” below, if you want to do that.)

Check that the **inetd.conf** file located in **\$OPENNT\_ROOT/etc** has the correct file permissions on it (we suggest mode 644: read and write permission for owner, read permission for group and world).

---

## Security and Inetd

Many systems run **inetd** and the other r-daemons as “root,” a special user with unlimited privilege. In particular, the r-daemons (**rshd**, **rexecd**) use the **.rhosts** file to allow access with very little authentica-

tion—there is no password checking. Both of these practices are inherently insecure.

The problem with running **inetd** as root is that allowing utilities to run with unlimited privilege is a dangerous practice. To reduce the potential for security exploitation, Windows NT provides different levels of privilege (there is *no* “root” user). Softway Systems advocates that the **inetd** and r-daemons be run with the minimal set of privileges required. They *could* be run as Administrator, but the Administrator account has additional privileges not required by **inetd**. Thus, we recommend creating a special user account which will run the **inetd** server with the minimal set of privileges.

The inetd user does not need to part of a domain-wide group; you can create a local user for **inetd**. See below for a discussion.

Many systems use the “root” user (an unlimited-privilege user) to allow particular utilities to perform fundamental security checks and to allow security checks to be bypassed for convenience’s sake.

The **.rhosts** file was a mechanism used to allow users remote access to a system without specifying a password. This type of mechanism is a security threat and is the reason why many systems have disabled these utilities. On Windows NT, all access must be authenticated (that is, a password is always required).

For those who want the “traditional” (no password required) behavior, the INTERIX remote daemons have been modified to look for a file **.password** in the user’s home directory. This file contains the user’s password and is used to create the login process for that user.

**Note:**

Softway Systems does *not* recommend using the **.password** file, but it is provided for those who need the behavior. A more secure mechanism for achieving the same end may be provided in a future release of INTERIX.

For **rsh**/**rlogin**/**rcp** to accept a login without prompting for a password, it is the **inetd** process that queries the **.password** file. Thus, this file must allow read access to the user account that is running the **inetd** process.

The permissions required on the **.rhosts** file are the usual ones: The file must **not** be writable by anyone other than the owner. Traditionally, this is mode 600.

The permissions required on the **.password** file are the same as the **.rhosts** file, **plus** the file must be readable by the account running **inetd**.

So we recommend creating the user “inetd” to run **inetd** because:

- It reduces the number of privileges needed to the minimum.

- It provides a domain-wide account to provide the same service. This reduces the administrative overhead for properly configuring several **inetd** accounts.
- All users can have a single additional Windows NT Access Control Entry (ACE) on their **.password** files that works across the domain.
- It is an account that should **not** ever need be used by members of the Administrators group. The minimal privileges on the “inetd” account minimize the chance that the account will be used for other chores, accidentally jeopardizing security.
- Because the **.password** file is readable by the “inetd” user, having the inetd account not used by a human reduces the chance of someone peeking.

We also recommend assigning the “inetd” account a long, complex and difficult password. This will reduce chances of someone breaking the account’s password. Since it is not an account used by a human the password need not be easy to remember or type or be short.

## Why a Domain User Account?

You only need to set up a domain user account to run **inetd** if:

- Users’ home directories are on shared filesystems, such that any user can login from any machine and be placed in the same home directory; *and* either of the following two reasons:
- You want to provide users with the ability to login without supplying a password, using the **.rhosts** and **.password** mechanism; or
- You have so many machines that it is much faster and more convenient to set up a domain account instead of creating one on each machine.

Otherwise, the user account which runs **inetd** can be a local account on the machine. With a workgroup configuration, the user account must be a local account, because security authentication is not shared between machines.

Consider a network with users’ home directories on a shared filesystem on the Primary Domain Controller, drive **//M/**, and the machines Huey, Dewey, and Louie:

User Anna on Huey uses **rlogin** to connect to Dewey. The **rlogind** program is invoked by **inetd** and runs as that user. The **rlogind** program on Dewey checks to see that the inetd user account has permission to read the **.password** file in **//M/users/home/anna**.

Now Anna uses **rlogin** to connect to Louie. The **rlogind** program on Louie checks to see if the inetd user account has permission to read

the **.password** file. Because this is a domain user account, the same user is running **rlogind** in both cases.

Now consider the same situation with *local* inetd user accounts. The account running Dewey's **inetd** is not the account running Louie's **inetd**; Anna's **.password** file must have special permissions for both Dewey's inetd user account and Louie's inetd user account. On a large network, this could require the administrator to set up special permissions for twenty, forty, or a hundred different inetd user accounts on each **.password** file.

By using a domain user account, all **.password** files are accessible to the account running inetd in that domain. The administrator needs to set up only a single account and each **.password** file needs only permissions for the user and the domain account running inetd.

If home directories are not shared, only the machine with the user's home directory will have access to the user's **.password** file. This is ideal for a configuration where you want users to be able to **rlogin** or **rsh** to their home machine from anywhere in the network.

## The Account Running inetd on Workgroups

In a workgroup, user authentication is not shared between machines. Each machine in a workgroup must have a local inetd user account.

Because workgroup machines do not have domains, you must specify the domain as empty. For example:

```
$ rlogin -l +ann Huey
```

You can also set a default login domain for a particular machine by setting a registry entry. This is part of the **login** command, and is documented on the **login** reference page.

---

## Overview: Setting Up Inetd

These are the steps for readying your network and system for **inetd**:

- ☐ On the primary domain controller for the network, create a new user named "inetd" as specified in this paper. This only needs to be done once.

- ❑ On each machine which will run **inetd**, the users' home directories must be located on an NTFS file system. This is a security measure. If the home directories are on a FAT file system, security is minimal and the **in.rshd** and **in.rlogind** daemons will not use the **.rhosts** or **.password** files. The **rsh** command will not work. The **rlogin** command will always require a password.
- ❑ If the machine has a separate **telnetd** service running, disable it using the **service** command. (After installing and setting up **inetd**, the **telnetd** daemon no longer needs to be started as a service; instead it is started by **inetd**.)
- ❑ On each machine, start **inetd** as a service. See "Start inetd as a Service," below.
- ❑ On each machine, start **syslogd** as a service to gather messages from daemons (See "Start syslogd as a Service," below, and see the **syslogd** man page for more information).

## Creating the inetd Account

Before installing **inetd** service, we recommend you create a new user account named "inetd" in the primary administrative domain. This must be done on your server, but it only needs to be done once. Workstations on the network will have access to the "inetd" account through the primary domain controller.

The "inetd" user requires at least one privilege and needs to belong to at least one group. We recommend this one group be create specially for **inetd** and this group have the one special privilege of "Logon Locally". By running **inetd** as a user with the fewest possible privileges, the potential security risk is significantly reduced.

Here is a step-by-step example of setting up the "inetd" account correctly as a domain account. It makes use of the "User Manager for Domains" program found on NT Server.

**To create a local "inetd" user**, use the "User Manager" program. Wherever these instructions say "Global" (for example, "New Global Group"), substitute "Local" ("New Local Group").

Assume that the administrative domain is named "accounting" and the machine that serves this domain is named "server1". Substitute as appropriate for your site.

- 1) Logon to server1 as Administrator and start the program "User Manager for Domains":
  - On **NT 4.0** "Start->Programs->Administrative Tools->User Manager For Domains"
  - On **NT 3.51** "Program Manager->Administrative Tools->User

Manager For Domains”

2) Create a new group:

- a) Select menu item “User->New Global Group”.

A window titled “New Global Group” will open.

- b) Fill in the New Global Group box:

- For Group Name, enter “Local Logon”.
- For Description, enter “Local Logon Privilege Only”.
- If any members are listed in the *Members* box, remove them.
- Click on “OK”.

The window will close.

3) Set the user rights for the new group:

- a) Select menu item “Policies->User Rights”.

A window titled “User Rights Policy” will open.

- b) From the “Rights” box pull-down, select the privilege “Log on locally”.

- c) Click on “Add”.

A new window will open titled “Add Users and Groups”.

- d) Click on the group entry “Local Logon”.

- e) Click on “Add”.

- f) Click on “OK”.

The window will close and you will go back to the previous window “User Rights Policy”.

- g) Click on “OK”.

The “User Rights Policy” window will close.

4) Create the “inetd” user:

- a) Select menu item “User->New User”.

A window titled “New User” will open.

- b) For Username enter “inetd”.

- c) Fill in the remaining boxes as needed for your site. Your policies may differ, but we recommend:

Give this “inetd” account a long, complex and difficult password. This will reduce chances of someone “breaking” the account’s password. (Since the password is only used once to set

up the service, it doesn't need to be easy to remember or type.)

Don't disable the account (leave Account Disabled unchecked).

Don't require the user to change the password at next login.

Do check the "User cannot change password" box.

Do check the "Password will never expire" box.

- 5) Set group memberships so that user "inetd" belongs only to the group "Logon Local":
  - a) Click on "Groups". A window titled "Group Memberships" will open.
  - b) Select group "Logon Local" from the "Not Member of" list.
  - c) Click on "Add".
  - d) Select group "Logon Local" from "Member of" list.
  - e) Click "Set". This will set "Logon Local" as the user's primary group.
  - f) Select and remove all other groups from the "Member of" list.
  - g) Click on "OK". The window will close and you will go back to the previous window "New User".
- 6) Click on "OK". The window will close.
- 7) Exit User Manager For Domains.

## Start inetd as a Service

Once the "inetd" account has been created for the domain and the files installed on the machine, **inetd** may be installed as a service.

It may be installed to start automatically when the system is booted, with the example below.

- 1 Login as Administrator.
- 2 At an INTERIX **ksh** or **csk** prompt enter:
 

```
% service install -u inetd -s auto -p inetdpassword \
$OPENNT_ROOT/usr/sbin/inetd -s
```

Replace "*inetdpassword*" with the correct password. If you do not want the service to start automatically, omit the "auto" from the command line.

- 3 Start the **inetd** service:
 

```
% service start inetd
```

It's sometimes necessary to wait a moment after installing the service before starting it.

## Start *syslogd* as a Service

To record messages from **inetd** and other daemons, you may install and start **syslogd** as a service.

It may be installed to start automatically when the system is booted, with the example below.

1 Login as Administrator.

2 At an INTERIX **ksh** or **csk** prompt enter:

```
% service install -u Administrator -p adminpasswd \
-s auto $OPENNT_ROOT/bin/syslogd -s
```

Replace “*adminpasswd*” with the Administrator’s password. If you do not want the service to start automatically, omit the “auto” from the command line. Both **-s** flags are required.

3 Start the service:

```
% service start syslogd
```

It’s sometimes necessary to wait a moment after installing the service before starting it.

---

## Disabling a Daemon

You may wish to disable or “turn off” one or more of the daemons. To do this, login as Administrator and edit the **inetd** configuration file, **\$OPENNT\_ROOT/etc/inetd.conf**. Place the comment character “#” in the first column of the line listing the daemon you wish to turn off. Then save the file. Remember to check that file permissions are correct for security reasons (mode 644, “rw-r- -r- -”).

---

## Specific Daemon Notes

The utilities and daemons in this package are ported from traditional Berkeley sources, so they behave as you might expect. There are some differences, described here.

### ftpd

This **ftpd** does not allow the use of “anonymous” connections. This has been disabled for this pre-release version of the daemon package.

### inetd

As documented elsewhere in this paper, we recommend **inetd** should be from a special “inetd” account. This is for security reasons. There is

no reason to run **inetd** as “Administrator” or any other group or user with more than “Log on locally” privilege.

Note that in the **inetd.conf** file the “user” column has “NULL” in it. INTERIX **inetd** ignores this column for the same security reason listed above. This column is maintained in the configuration file for portability.

## ntalkd

The protocol for **talk** is that user names are at maximum 11 characters long followed by a terminating “\0” (NULL). The protocol can’t be extended for longer names. Long character names which are not unique until after the 11th character present problems—both “Administrator” and “administrator3” will match. In this case, specify the *tty* argument with your **talk** request.

**Ntalkd** matches usernames in a case-independent manner since the canonical user name may not be in the case expected by the caller. This is similar to mail protocols and should therefore be more like what the user expects.

## rdist, rdistd

INTERIX doesn’t yet support symbolic links, so **rdist** and **rdistd** do not support symbolic links. Always use the option **numchkgroup** because Windows NT group names may contain spaces. Spaces confuse the rdist protocol.

## rcp, rlogin, in.rlogind, rsh, in.rshd

These utilities and daemons make use of the files **.rhosts** and **.password** (the **.password** file is an INTERIX extension). If the permissions on these files are not correct, the programs will not use the contents of the files.

By default, the supplied **inetd.conf** file has **in.rlogind** start with the **-a** option, which asks for hostname verification.

If you do not want **.rhosts** files to be read in any case, edit **inetd.conf**: For **in.rlogind**, add the **-l** option after the **-a**. For **in.rshd**, add the **-l** option after the **-a** option.

INTERIX does *not* install a **hosts.equiv** file. If you want a **hosts.equiv** file, you must create it yourself. The file should reside in **\$OPENNT\_ROOT/etc**. The file must be a regular file. It’s permissions should allow the world to read but not write it. The file’s group may be allowed to read it but cannot write to it. The owner may be anyone.

If **hosts.equiv** is *not* a regular file, and is writable by either the file's group or the world, the file will be ignored.

For specifics of correctly setting the **.password** file see the "Note for Users of rlogin, rsh and rcp" below or the man page for **rlogind** or **rshd**.

When logging into another system, the **rlogin** and **rsh** clients use your username *without* a Windows NT domain as both the remote and local username. (For example, "ADMIN+cday" becomes "cday".) When connecting with another INTERIX system, the domain name is useful, especially if you're using **.rhosts** / **.password** files. The clients have been extended to take a **-D** option, which leaves the Windows NT domain name in the remote and local usernames. If you also use the **-l** option, the argument to **-l** always takes precedence as the remote username.

## talk

**Talk** ensures that the requesting user's username is all in lower case. The target user's username is left as written on the command line. This is done to ensure maximum compatibility with other **talk** daemons and makes users on other systems happier when they connect for the **talk** session.

## telnetd

In OPENNT 2.0 and 2.1, the default behavior of **telnetd** was changed so that **telnetd** ran effectively as a service, not as a daemon. To run it as a daemon under **inetd**, the INTERIX version of **in.telnetd** must be invoked with the **-i** ("inetd") option. If you make changes to the **inetd.conf** file ensure that the **-i** option accompanies **telnetd** in the last column, as specified on the **telnetd** man page.

## tftpd

By default, **in.tftpd** is disabled in the **inetd.conf** file. If you want to activate **in.tftpd**, read the reference page first. There are security concerns.

---

## Note for Users of rlogin, rsh and rcp

Traditionally on systems supporting the **rlogin** and **rsh** daemons, you only need a correctly configured **.rhosts** file in your home directory to have **rlogin**, **rsh** and **rcp** work. Because security is different on Windows NT, if you want to do an **rlogin** / **rsh** / **rcp** into an INTERIX system

without being prompted for a password, you require an additional file, the **.password** file, in your home directory.

**The .password file only works if it resides on an NTFS file system.**

The reason for this is that security cannot be maintained on a FAT file system. If your home directory is on a FAT file system, you cannot set the permissions correctly on the **.password** file.

To maintain security, use the utility **regpwd**, supplied as part of the daemon package. This utility creates or replaces the user's **.password** file and sets the correct security permissions on the file. Use **regpwd** to create or update the contents of the **.password** file.

**Note:** Do *not* use **chmod** to adjust the permissions on the **.password** file. **Chmod** will reset certain permissions, and you will need to use **regpwd** again.

The following is an example of using **regpwd** to create a **.password** file. In this example, **inetd** is being run by the user "inetd" in the domain "accounting". Each person who wants to use **rcp**, **rsh**, and **rlogin** with a **.rhosts** file should follow these instructions:

- 1) Start **regpwd**, supplying the domain and username of the user running **inetd**:

```
$ regpwd accounting+inetd
```

You do not need to be in your home directory. The **regpwd** program prompts you for your password.

- 2) Enter your password. It will not be echoed to the screen.

When the program has successfully completed, it writes to the screen:

```
processed file: C:\home\mary\.password
```

Otherwise, **regpwd** exits with an error message.

- 3) Create or adjust a **~/rhosts** file which contains the names of hosts from which you may login. The format of the entries in the **.rhosts** file is:

```
hostname [username]
```

The *username* can be left off if your username on the machine *hostname* is the same as your username on the machine containing the **.rhosts** file.

**Note:** When creating a **.rhosts** file on a remote machine which is *not* running INTERIX, you will need to specify your *username* as *domain+username*, or use the **-l** option with **rlogin** and **rsh**.

- 4) Set the permissions on the **.rhosts** file correctly using **chmod**:

```
$ chmod 600 .rhosts
```

## Testing the .password File

To test that the **.password** file is usable and correctly configured, go to another machine (or use **telnet**, if that machine has a working **telnetd**) and use **rlogin** to login to the machine. If you are prompted for a password then something is not correct. Check the following:

- Is the hostname of the machine where you are running **rlogin** or **rsh** in the **.rhosts** file? You may need to use the fully-qualified domain name.
- Is your password correct in the **.password** file?
- Are the permissions correct on the **.rhosts** file (mode 600)? Check using **ls -l**.
- Are the permissions correct on the **.password** file (mode 600, plus one ACE for the **inetd** user)? Check using **CACLS.EXE**.
- Was the correct user specified with the additional ACE? Check using **CACLS.EXE**. The command output should list 4 ACEs, one each for the **inetd** account, the file's owner, the group, and Everyone.
- Was the **inetd** username given to you correct?
- Is **inetd** running as the correct username? Check using a command such as:

```
% ps -e -o pid,comm,user=longtitlesolongnamesprint
      PID COMMAND                                longtitlesolongnamesprint
      65536 //E/OpenNT/bin/cron1                  accounting+jo
      65537 ksh.exe                               accounting+jo
     1507330 ps                                    accounting+jo
     1114115 inetd                                accounting+inetd
```

- Is your home directory on an NTFS file system? Use **df** to check; the entry in the "Type" column should be **ntfs**:

```
$ df ~
Filesystem                                [...] Type  Mounted on
//Mordred/c_drive                        [...] ntfs  //M/
```

- Check the owner of the file using **ls -l**. Is it owned by you? If it is owned by another user, a security problem has occurred. Record the file information (the **.password** file's time, date, and owner). Immediately change your password, and report the security problem to your senior systems administrator. He or she should re-

spond to this incident as a serious matter.