Talis Assist Security

System Manager Guidelines

April 2009

About this document

- This document provides guidelines for managing the security features set up as part of secure Solaris server builds to help protect the system from unauthorised access.
- It is intended for System Managers who use the Talis Assist Security service.
- Knowledge of UNIX, the Talis LMS, and a very basic understanding of network and security fundamentals is assumed.

Talis Support

If you are experiencing difficulties, please contact your System Manager/IT Department in the first instance.

You can now raise, track, and close your support cases using Talis' 24 x 7 **My Support** web service. You must have a user name and password to access the service – you can register at the following address: http://www.talis.com/services/register/index.shtml

Talis Support Site: http://www.talis.com/services/support/

Telephone: +44 (0)870 400 5400

Email: support@talis.com

Copyright notice

Contents (right-click to update)

1. Solaris IP-Filter firewall

The server will be configured with a host based firewall to restrict access and block ports that are not commonly used in a Talis environment. Services such as Alto and shell access will usually be tied down to your local network, with TCP wrappers available to further restrict access where necessary.

1.1 Configuration files

The firewall uses two configuration files to define allowed access:

/etc/ipf/ipf.conf Main configuration file
/etc/ipf/ipnat.conf NAT (unused) and Special protocol handling (FTP)

1.2 Log files

The firewall logs to the following files:

/var/adm/messages Errors with starting the ipfilter service
/var/log/ipflog Blocked packets (where log is specified in ipf.conf)

1.3 Common tasks

The following commands can be used to inspect or re-load the configuration from the above files when logged in as the root user:

ipfstat -ioh Show rules including match counts
ipf -Fa -f /etc/ipf/ipf.conf Re-load configuration from ipf.conf

Note: You should update the tripwire database after making changes (see Tripwire section of this document). You can only accept or decline all of the suggestions.

cd /tripwire
tripwire -update /etc/ipf/ipf* Update the tripwire database to reflect changes

1.4 Allowing access from new IPs or Subnets

Here is an example of adding a new entry for Alto access

```
cd /etc/ipf
cp ipf.conf ipf.conf.`date +%Y%m%d%H%M`
vi ipf.conf
```

Find the appropriate section, in this case "Talis Alto". The section will usually have one or more lines with the same IP or subnet address. You will need to duplicate a full set of lines and change the IP or Subnet address as required with optional comments.

original lines:

```
## Talis Alto
pass in quick proto tcp from 10.0.0.0/8 to any port = 2025
pass in quick proto tcp from 10.0.0.0/8 to any port = 210
pass in quick proto tcp from 10.0.0.0/8 to any port = 211
```

additional new lines (for 192.168.2.0/255.255.255.0):

```
# new branch library staff subnet
pass in quick proto tcp from 192.168.2.0/24 to any port = 2025
pass in quick proto tcp from 192.168.2.0/24 to any port = 210
pass in quick proto tcp from 192.168.2.0/24 to any port = 211

# new branch library staff subnet (shorter format, same as above)
pass in quick proto tcp from 192.168.3.0/24 to any port = 2025
pass in quick proto tcp from 192.168.3.0/24 to any port 209 >< 212
```

You can activate the changes using the ipf command mentioned earlier.

2. How to update TCP wrapped services

2.1 Allowing access from new terminals

Here is an example of adding a new terminal for telnet access

cd /etc
cp hosts.allow hosts.bak.`date +%Y%m%d%H%M`
vi /etc/hosts.allow

Add a line to the end of the file as follows with optional comment. You can also append to an existing line (if it makes sense).

 # insert comment here
in.telnetd: 10.10.10.1 172.16.0.3

Tip: Run "tcpdchk" before and after your change and correct any new errors or warnings (not available on Solaris 10). Failed name lookups and no sshd process can be ignored.

2.2 Allowing temporary access to services

Here is an example of adding a new terminal for temporary access:

cd /etc
cp hosts.allow hosts.bak.<ddmmyy>
vi /etc/hosts.allow

Add a line to the end of the file as follows (or append if line exists).

 # temp access for xyz
in.telnetd: 10.10.10.1 172.16.0.3: severity warning

Temporary FTP Access

 # temp FTP access for xyz
in.ftpd: 10.10.10.1 172.16.0.3: severity warning

This will allow the connection but log it with a warning in the system authlog file to help remind you to disable it

Note: If this is a re-occurring event you can insert a **#** before the above line to disable the access until it is needed again.

Tip: Run "tcpdchk" if on Solaris 8 before and after your change and correct any new errors or warnings. Failed name lookups and no sshd process can be ignored.

3. Troubleshooting Access problems

To checking if an access problem is with the server you should open two connections to the server from a PC you have access from and run the following commands, one in each window:

tail -f /var/log/ipflog
tail -f /var/log/authlog

Hit <ENTER> a few times to add some blank lines to the bottom of your screen and then try connecting from the problem PC.

If you get a new line in **ipflog** that has the IP address of the affected PC you need to update **ipf.conf**.

```
Jun 18 11:03:51 xxtalis ipmon[xxx]: [ID 702911 local0.warning] 11:03:50.947507 e1000g0 @0:58 b
10.1.49.150,3072 -> 172.30.10.3,21 PR tcp len 20 48 -S IN
```

If you get a new line in **authlog** you need to update **/etc/hosts.allow**.

```
Apr 27 15:48:37 xxtalis sshd[xxx]: [ID 947420 auth.notice] refused connect from 10.1.49.150
```

You could fix this by adding this line to the end of the System Administration section in **/etc/ipf/ipf.conf**:

pass in quick proto tcp from 10.1.49.0/24 to any port 20 >< 24 keep state

Apply the changes:

ipf -Fa -f /etc/ipf/ipf.conf

Then add the specific IP to /etc/hosts.allow for FTP:

in.ftpd: 10.1.49.150

You can choose to use add either the subnet or the IP in each case depending on if DHCP is in use and how secure the network in question is. If you have several IPs on the same subnet, typically it's simpler to add the subnet to ipf.conf and then the individual IPs to hosts.

4. Logcheck Messages

Logcheck is a software package that is designed to automatically run and check system log files for security violations and unusual activity. This will extract interesting and unusual activity in the logs and email it to the system administrator.

If logcheck detects potential hacking activity it will change the subject header to include "ACTIVE SYSTEM ATTACK". This should be reported to the Talis Helpdesk immediately.

There are three sections that will be reported if there is any information relative to that section:

- Active System Attack Alerts
- Security Violations
- Unusual System Events

4.1 Active System Attack Alerts

This section will contain messages that are usually generated by an active attack against the system. These messages should be treated seriously as they are unlikely to be false alarms.

4.2 Security Violations

This section covers issues that are security related such as repeated login failures or attempts to connect from unauthorised IP addresses. These may be a hacking attempt, a new terminal or user error. A single attempt to connect to the system can usually be ignored, as it may be accidental. A hacking attempt usually involves many attempts by the same source to multiple services. In the event of such activity you should report it to your network security department as other systems on the network may also have been targeted.

Below is an extract of a connection attempt, which takes the format of:

```
Oct 29 12:00:18 libtalis in.ftpd[25103]: [ID 947420 auth.warning] refused connect from
192.168.0.1
```

```
<date> <hostname> <service> [process id] <log label> refused connect from <source
IP/host>
```

In the above example we can see that a connection attempt was made by '192.168.0.1' to connect to the ftp service on the 'libtalis' server. Below is an extract of another message that you may encounter:

```
Jul 24 08:46:43 libtalis login: [ID 376080 auth.crit] change password failure:
Permission denied
```

When a users password has expired the user is prompted to enter a new password when he/she tries to login. The new password MUST differ by at least three (3) characters, MUST be alphanumeric and at least PASSLENGTH (see /etc/default/passwd) characters long. If the user managed to get it wrong 3 times the connection will be closed and the above message logged.

5. Unusual System Events

All other messages are checked and reported in this section unless they have been added to the logcheck.ignore file. Most of the known messages generated by usual activity on Talis LMS servers have been added to this ignore filter.

Examples of messages in this section are below:

```
Jul  8 07:57:23 libtalis sshd[205]: [ID 800047 auth.info] Server listening on :: port 22.
Jul  8 07:57:23 libtalis sshd[205]: [ID 800047 auth.info] Server listening on 0.0.0.0 port 22.
```

The above example is generated by the SSH daemon when it is started usually when the system is rebooted. The system administrator can check the time against known system reboot times and any other work that may involve restarting the daemon and ignore it otherwise further investigation should be done.

5.1 Suppressing false alarms and specific re-occurring messages

If you have repeated false alarms or want specific errors ignored, you can reconfigure logcheck to ignore these.

There are two files that make up the ignore filter:

/usr/local/etc/logcheck.violations.ignore
/usr/local/etc/logcheck.ignore

5.1.1 logcheck.violations.ignore

This file controls what is ignored in the "Security Violations" section. Changes to this should ideally be done through the Talis Helpdesk to ensure you do not ignore important messages.

For example, to ignore the following message (which may already be done):

```
Jul  9 14:00:02 libtalis in.rshd[29584]: [ID 927837 auth.info] connect from localhost
```

Add the following line to logcheck.violations.ignore:

in.rshd.*connect from localhost

5.1.2 logcheck.ignore

This file controls what shouldn't be displayed in the "Unusual Activity" section. It contains regular expression patterns that we should ignore if found in a log file. If you have repeated false alarms or want specific errors ignored, you should put them in here. Once again, be as specific as possible, and go easy on the wildcards.

For example, to ignore the following message that may occur if your DNS is unavailable or not configured:

```
Jul  9 18:25:10 libtalis sshd[4296]: [ID 800047 auth.info] Could not reverse map
address 194.80.16.2.
```

Add the following to logcheck.ignore:

sshd.* Could not reverse map address 194.80.16.2

6. Tripwire and the tripwire Databases

There are two tripwire databases, the full database includes a fingerprint of every file on the system and the system database includes a subset of important system files to detect early hacking attempts.

The smaller system database resides in '/var/tripwire/databases/tw.db_<hostname>'.

The full tripwire database resides in '/var/tripwire/databases/tw.db_hostname.full.gz'.

When logcheck reports that files have changed and these are known legitimate changes affecting a few files you will need to update the system database to reflect these (see updating database instructions below).

If there is a major change, such as a Talis software upgrade, you will need to initialise the full database (see re-initialise instructions below).

6.1 Updating the system tripwire database

When a legitimate change is made to system configuration files such as '/etc/hosts.allow' to add new terminals, the database needs to be updated to reflect the change.

Login as the root user

cd /var/tripwire
tripwire –update /etc/hosts.allow

Multiple files can be specified on the same line.

6.2 Updating the tripwire configuration file for the system database

Edit the '/usr/local/etc/tw.config' file and in the 'General Excludes' section of this file add files or directories that you do not want tripwire to check

Example of a log file to be excluded:

```
# General Excludes
!/etc/lu/lustartup.log
```

Further examples are included in the above configuration file.

♦

Note: Ensure that important system binary files are not excluded.

After editing the configuration file update tripwire database. Below is an example of an update after a change to the configuration file:

cd /var/tripwire
tripwire -update /usr/local/etc/tw.config /etc/lu/lustartup.log

6.3 How to initialise the full tripwire database

When legitimate changes, such as software upgrades are made to the files the full tripwire database will need re-initialising to reflect these changes.

To initialise the full tripwire database run the following script logged in as root.

/usr/local/bin/tw-init-full

Talis recommends running a full_ufsdump or full_softdump to archive the database, as the integrity of the disk copy cannot be guaranteed in the event of a compromise.

6.4 How to initialize the system tripwire database used in daily checks

To initialize the system tripwire database run the following commands logged in as root:

cd /var/tripwire
tripwire -init

Talis recommends running a full_ufsdump or full_softdump to archive the database, as the integrity of the disk copy cannot be guaranteed in the event of a compromise.

7. Changing the list of users with SU access

Only members of the admins group have access to the 'su' command.

To add or remove users, edit the /etc/group file. User names are comma separated with no spaces (white space) between users or commas.

vi /etc/group

For example:

admins::11:ops,report

8. Changing the list of email report recipients

To add or remove email addresses, edit the /etc/mail/aliases file. Email addresses are comma separated.

vi /etc/mail/aliases

For example:

sysman: J.Bloggs@library.gov,J.Doe@library.ac.uk

When you have made the changes and saved the file, run **newaliases** to update the mail aliases database.

newaliases

9. Changing the IP addresses that can access Webmin

The Webmin server can be configured to deny or allow access only from certain IP addresses. You should limit access to your server to trusted addresses, especially if it is accessible from the Internet. Otherwise, anyone who guesses your password will have complete control of your system.

9.1 Connect to Webmin using a Web browser.

Click on the "Webmin Configuration" icon and then click on the "IP Access Control" icon. The "Only allow from listed addresses" radio button should already be selected.

Add network/host IP addresses, one per line, to allow access from and then click on "save"

For example:

```
10.254.3.0
10.254.1.0/255.255.255.128
```

Note: may also need to update the IP Filter firewall configuration.

10. How to use “John” the Password Cracker

Talis recommend running the password cracker once a month.

Log in as the root user.

If the following files exist in **/usr/local/run** then remove them:

- restore
- john.pot

Execute the following command:

/usr/local/run/john /etc/shadow

The password cracker should find any weak passwords within the hour. It can be terminated after an hour of running by holding down the 'Ctrl' key and pressing 'C'.

Below is an example of the cracked passwords. The first column shows the cracked password and the second column shows the account name.

Loaded 25 passwords with 25 different salts (Standard DES [32/32 BS])

abc123 (talis)

jbloggs (jbloggs)

xyz123 (xyz)

11. Securing the Hardened server with ufsdump or fs_dump.sh

Talis system manager documentation advises that the system is backed up using full_softdump. Users should continue to use this or any custom solutions already in place to secure the Talis software according to their regular schedule.

We have found that restoring Server Hardening is easier and quicker from a UFS based file-system dump. Therefore we would encourage users to perform an ufsdump after significant changes to the Server Hardening or operating system alongside the full_softdump. Significant changes include patch updates and Solaris upgrades. To help with this we have created the full_ufsdump.sh and fs_dump.sh scripts that will dump all the local UFS (and ZFS for fs_dump.sh on Solaris 10) file-systems on the server.

An advanced release of full_ufsdump.sh / fs_dump.sh is planned in the near future, which will officially make full_softdump obsolete/redundant. This will be made available to the wider customer base.

To secure your server use the following logged in as root:

 # Solaris 8:
/usr/local/bin/full_ufsdump.sh [device]

 # Soalris 10:
/usr/local/sbin/fs_dump.sh [device]

Where [device] is an optional Unix tape device. If it is not specified the "/dev/rmt/0hn" device (full_ufsdump.sh) or "/dev/rmt/0cn" (compressed device for fs_dump.sh) will be used. To dump a client's file-system to a remote server's tape drive you can do the following

/usr/local/sbin/fs_dump.sh [server:]<device>

For example:

/usr/local/sbin/fs_dump.sh libserver:/dev/rmt/0cn

12. Selecting Good Passwords

12.1 Rationale

The object when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about what you've chosen. This leaves him no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a machine that could try one million passwords per second (most machines can try less than one hundred per second), would require, on the average, over one hundred years to complete.

12.2 What Not to Use

- Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your spouse or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than six characters.

12.3 What to Use

- Do use a password with mixed-case alphabetic characters.
- Do use a password with non-alphabetic characters, e.g., digits or punctuation.
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.
- Method to Choose Secure and Easy to Remember Passwords
- Choose a line or two from a song or poem, and use the first letter of each word. For example, ``In Xanadu did Kubla Kahn a stately pleasure dome decree" becomes ``IXdKKaspdd1."
- Alternate between one consonant and one or two vowels, up to eight characters. This provides nonsense words that are usually pronounceable, and thus easily remembered. Examples include ``r0utboo," ``quadp0p," and so on.
- Choose two short words and concatenate them together with a punctuation character between them. For example: ``d0g;Ra1n," ``b0ok+Mug," ``k1d?G0at."

Excerpts from:

IMPROVING THE SECURITY OF YOUR UNIX SYSTEM

David A. Curry, Systems Programmer

Information and Telecommunications Sciences and

Technology Division

ITSTD-721-FR-90-21