Preserving and Restoring iTools Configuration

Tenon Intersystems

This contains a description of the files and scripting needed to preserve and recover an iTools installation.

The basic steps to creating an iTools installation, based on a previously installed iTools, are relatively straightforward:

- Preparation - Configuration and testing of the new machine.
- Backup - Backup the existing configuration.
- Restore - Restoring the saved configuration.

This document contains a framework for each of these steps.

Preparation

In prepration for the backup of the iTools files, make a note of the various packages that you have installed. Allocate a few hours to do the migration and warn your customers of possible unexpected downtime in case something goes wrong.

PREPARING THE NEW MACHINE

If migrating your iTools installation to a different machine, prepare that machine for installation by installing the latest version of Mac OS X Server applying any Apple update that may be available. Also, install the latest version of iTools.

After you have finished installing Mac OS X Server and iTools on the new machine, you should test the server's basic functionality. Such items include, but are not limited to:

- Can you access the default web page?
- If you are planning to run an SSL site, is the SSL package installed, and can you create a temporary (test) certificate?
- Can you access the iTools admin server successfully?

You will have to decide how you will transfer the files to the new machine from the old one. This paper will discuss creating a "tar.gz" archive that can be sent by FTP to the new machine, but you can also use any number of methods including Apple File Sharing, NFS, and other methods.

PICK A DESTINATION

In order to prepare to back up iTools, you must first find a target to back up onto. The target could be a mounted Apple File Sharing drive, an NFS drive, or another hard drive in the machine. The instructions given can be easily adapted to backing up and iTools installation instead ofmigrating iTools to a new machine.

Files to Save and Restore

This step involves determining what iTools components you have installed, and then determining what files to back up. Based on this information, you can construct an archive file that can be moved to the new machine or backed up to another disk.

If you do not know which iTools components that you have installed, you can check the “/Local/Library/WebServer/tenon/logs/iTools.updates” file. This file contains a log of all of the iTools components that are installed. It also contains a record of the time and date at which each particular component was installed.

The main iTools package consists of a number of components including the Apache server, the Squid object cache, FTP (wu-ftpd), sendmail, BIND, and the admin server. Listed below are the files associated with each component and a description.

APACHE SERVER

/Local/Library/WebServer/Configuration/apache.conf

apache.conf is the main Apache configuration file used with iTools. All new virtual hosts and Apache directives added with the admin server are placed in this file. This file is essential for operation of both iTools and Apache.

/Local/Library/WebServer/tenon/apache/conf/iTools.conf

iTools.conf is the secondary Apache configuration file used by iTools. It contains iTools-specific directives and is modified by the various installer scripts. It is important this file is saved because it contains changes and modifications made by the various installers. Failure to copy this file could result in certain iTools components (such as WebCatalog or WEBmail) not working properly.

/Local/Library/WebServer/Logs

Though not essential to web server operation, it may be desirable to save the Logs directory when backing up or migrating to an iTools installation on a new machine. Saving the files in this directory can help to maintain consistency if log analyzer utilities are used.

SQUID OBJECT CACHE FILES

/usr/local/squid/etc/squid.conf

squid.conf is the main Squid cache configuration file. It will contain, not only the current cache configuration parameters, such as the verbosity of the access log (whether or not referer or user-agent are logged), but also memory and disk cache size. If enabled, the squid.conf file will also contain IP-based access restrictions entered into the admin server. Failure to copy this file will result in loss of some access control settings, the cache stop list, and the various other Squid configuration parameters mentioned above.

FTP CONFIGURATION FILES

/etc/ftpaccess

ftpaccess is the main FTP server configuration file. It contains all virtual anonymous FTP directives, and also contains settings such as the maximum number of users allowed to log in and whether anonymous/user-pass FTP access is enabled in the admin server. Failure to copy this file will result in loss of these settings.

SENDMAIL CONFIGURATION FILES

/etc/sendmail.cf

sendmail.cf is the main sendmail configuration file. It is rarely ever changed. There is no need to save or backup this file unless you have changed this file.

/etc/sendmail.cw

sendmail.cw is a sendmail configuration file that contains a listing of the hosts for which sendmail is to receive mail for. It is recommend that you save this file if you have added virtual hosts. Each time a virtual host is added in iTools, this file is updated with the host and domain name of that host.

/etc/mail/relay-domains

relay-domains is a sendmail configuration file that contains a listing of the hosts for which sendmail is to relay mail for. A relaying situation would occur if you used your iTools machine as an SMTP server. A clean iTools install delivers a blank file, so save or backup this file if you have changed it.

BIND CONFIGURATION FILES

/etc/named

The named directory contains the BIND or DNS configuration db files. If you are using iTools as a DNS server, it is essential that you save this directory to maintain your DNS configuration. If not, this directory can be safely ignored.

MISCELLANEOUS ITOOLS CONFIGURATION FILES

/Local/Library/WebServer/tenon/libexec/iTools.sh

iTools.sh is the main startup script for iTools. It handles all of the necessary initialization functions and configures network IP addresses if you are using IP-based virtual hosts. This script generally runs once at system startup. Failure to copy this file could result in the failure of IP-based virtual hosts to function properly.

/Local/Library/WebServer/tenon/etc/license.info

license.info contains the license number information for iTools. Saving this file is important because a clean install of iTools loads a 14-day temporary license number. Once this license number expires, the Apache server in iTools will only operate for two hours at a time.

/Local/Library/WebServer/tenon/etc/users.db

users.db is an Apache database file that contains the usernames and passwords used by the "*Users*" section of the admin server and by Apache for verifying logins to password-protected pages. Since this file contains your admin password, it is very important.

/Local/Library/WebServer/tenon/etc/groups.db

groups.db is an Apache database file that contains the usernames and the groups they are associated with. This is used by the "*Groups*" section of the admin server and by Apache for verifying logins to realm-protected pages. Since this file contains the admin group and users allowed in this group, as well as any other realm-protected group access privleges, it is very important.

SSL PACKGE (DOMESTIC OR INTERNATIONAL)

The SSL package enables iTools to transmit information using the Secure Socket Layer (SSL). If you have this package installed and you are using SSL, then you will need to back up some of its associated files.

SSL KEY FILES

/etc/ssl/private

The private directory has severely restricted access permissions. The files contained within are only readable by the "*roo*t" user so they cannot be viewed by unauthorized users. The SSL key file is essential to SSL operation and is paired with the certificate. Loss of the key file will render your SSL certificate useless, so it is important to back it up. There may be more than one key file present if you have multiple IP-based virtual hosts with SSL enabled. The keys should be named <IP Address> key where <IP Address> is the IP address of the IP-based virtual host for which the key was created.

SSL CERTIFICATE FILES

/Local/Library/WebServer/tenon/ssl/certs/*.crt

Files with the .crt extension are SSL certificate files. They are matched with the key and are named <IP address>.crt where <IP address> is the IP address of the IP-based virtual host for which the certificate was created. Saving the certificate is as important as saving the key file.

OTHER SSL-RELATED FILES

/Local/Library/WebServer/tenon/ssl/certs/*.cnf

Files with the .cnf extension are SSL configuration files that contain the information that you entered when creating the certificate request (CSR) in the iTools administration server. These files are plain text files and are not required for SSL operation, but serve as a reminder of the settings that you used to create your certificate request (and certificate).

/Local/Library/WebServer/tenon/ssl/certs/*.csr

Files with the .csr extension are SSL certificate request (CSR) files. These files are what is given to your certificate authority so that they can make you an SSL certificate that matches up with the key generated internal by iTools. CSR files are not required for SSL operation, but should be kept in the case that the certificate becomes lost and the Certificate Authority (CA) needs to create a new certificate for you.

OTHER ITOOLS PACKAGES

For the most part, all other iTools package files are contained in the folder associated with that package. Configuration files that you have modified in association with each particular package should be backed up in a similar way to the iTools core and SSL package files.

Backing up files

The easiest and most effective way to manage backing up and moving the iTools configuration files is by using the *tar* command to tar up the configuration files and store them into a single file. This single file can then be moved to another machine and untarred to restore the configuration to the new system. The tar archive can also be moved to another disk or place of storage for backup purposes.

Tarring a set of iTools configuration files is as easy as following the format of the following command. Because different iTools users will be using different features of iTools, some users may need to back up more files than others. You should be able to add or remove Directory/File listings from the tar command given below.

BASIC TAR COMMAND

The easiest way to archive the files is to do it in a shell script. A simple shell script is included below. Note that the name of the archive can be changed to suit your individual preferences. You can create such a shell script by using any text editor on OS X Server. Remember to give your shell script execute permissions by issuing the command "chmod a+x <filename>" where <filename> is the name of the shell script. You can also use the OS X Server file browser utility to change the permissions on the file. You will also have to run this script as the *root* user if you want to back up your SSL key files in /etc/ssl/private.

```
#!/bin/sh
cd /
tar czvf itools-config-backup.tar.gz \
/Local/Library/WebServer/Configuration/apache.conf \
/Local/Library/WebServer/tenon/apache/conf/iTools.conf \
/Local/Library/WebServer/Logs \
/usr/local/squid/etc/squid.conf \
/etc/ftpaccess \
/etc/sendmail.cf \
/etc/sendmail.cw \
/etc/mail/relay-domains \
/etc/named \
/Local/Library/WebServer/tenon/libexec/iTools.sh \
/Local/Library/WebServer/tenon/etc/license.info \
/Local/Library/WebServer/tenon/etc/users.db \
/Local/Library/WebServer/tenon/etc/groups.db \
/etc/ssl/private \
/Local/Library/WebServer/tenon/ssl/certs/*.crt \
/Local/Library/WebServer/tenon/ssl/certs/*.cnf \
/Local/Library/WebServer/tenon/ssl/certs/*.csr
```

As we said, you may have to modify the files archived by tar to your own preferences. For example, if you do not have SSL installed, then you will not need or want to back up any files in the *tenon/ssl/certs* directory. If you have WEBmail Pro, you may want to back up the changes that you have made to your WEBmail by adding the */Local/Library/WebServer/web_mail* to the tar command. Remember the trailing "\" continuation character.

Restoring iTools Configuration

The next step in resotring an iTools configuration is to move the tar archive to the machine on which the files are to be restored. Once the tar archive is transfered to the new machine, move it to the root or "/" directory. Then execute the following command:

If iTools is running, first execute:

```
/usr/sbin/apachectl stop
```

```
tar zxvf itools-config-backup.tar.gz
```

This should extract all of the proper files to the right places. Then start Apache by typing:

```
/usr/sbin/apachectl start
```

You will have to restart all of your other services. This can be done by issuing the “ps ax” command and recording the process IDs (PIDs) for sendmail, named, and other processes (depending on what you have installed). Then send a HUP signal to those processes causing them to restart. This is done by issuing the command kill -HUP <PID> where <PID> is the process ID of the service that you wish to restart.

All should now be well with your web server. If something doesn't appear to be working correctly, restart your machine to make sure that you didn't accidently forget to “HUP” something. If you have any difficulties, check your log files. If you have trouble figuring out the log file, go back through all of these steps to make sure that you didn't miss something. If all else fails, send an e-mail to support@tenon.com who will be happy to assist you with any difficulties that arise.