Permissions and Ownership

Contents

- 1 Overview
- 2 Prerequisites
- 3 Symptoms
- 4 Solution
  - 4.1 Changing User Ownership
  - 4.2 Changing Group Ownership
  - 4.3 Changing Permissions
- 5 Default Permissions

Overview

Files and folders must have the correct ownerships and permissions to allow applications to run. This document covers what permissions are expected for some of the critical files. When they are upgraded, altered or moved it is important to ensure that permissions are retained.

These commands should not be attempted without first backing up Swivel.

Prerequisites

Swivel 3.x

Backup Swivel

Symptoms

Swivel may fail to start or exhibit issues such as graphical images failing to appear or error messages in the logs. Databases may be read only.

Solution

Changing User Ownership

A file ownership is listed by user and group. To change user ownership of a file use the *chown* command:

chown user filename

Example: *chown swivel config.xml*

the -R switch allows recursive files and directories

the command can also be used to change group by using:

chown user.group filename

Example: *chown swivel.swivel ./** changes all files in the directory

Example: *chown -R swivel.swivel ./pinsafe* changes all in the directory and subdirectories of Swivel (when run in webapps)

Changing Group Ownership

To change group ownership of a file use the *chgrp* command

chgrp group filename

Example: *chgrp swivel config.xml*

the -R switch allows recursive files and directories

Changing Permissions

Permissions of a file are defined as dashes or d for directory, r for read, w for write, x for execute (plus others we will ignore):

Directory: the first - or d for a directory d---------

User: -rwx------

Group: ----rwx---

Other: ------rwx

To change a permission use the chmod command:

chmod ugo+-permission filename

Example: *chmod ugo+r ./config.xml* gives read permissions to user, group and other.

Example: *chmod o-w ./config.xml* removes write permission from other.

Example: *chmod ug+rw ./** gives read and write permissions to all files and directories in the directory.

Care should be taklen with the wildcard (*) since directories and files have different permissions.

Default Permissions

These are listed in order to compare a system with what the default values are.

All files under <path to Tomcat>/pinsafe should be owned and members of the group swivel and generally have user and group read and write access, and read access for other.

i.e. -rw-rw-r-- swivel swivel filename

All directories under <path to Tomcat>/pinsafe should be owned and members of the group swivel and generally have user and group read, write, and execute access, and read and execute access access for other.

i.e. drwxrwxr-x swivl swivel directory

Verify ownership and permissions on the following system files, these are the ones that may contain incorrect ownerships and permissions:

/pinsafe/WEB-INF/conf -rw-rw-r-- swivel swivel config.xml

/pinsafe/WEB-INF/db -rw-rw-r-- swivel swivel derby.log drwxrwxr-x swivel swivel pid drwxrwxr-x swivel swivel swivel

/pinsafe/WEB-INF/db/pid and /pinsafe/WEB-INF/db/swivel -rw-rw-r-- swivel swivel dbex.lck drwxrwxr-x swivel swivel log drwxrwxr-x swivel swivel Seg0 -rw-rw-r-- swivel swivel service.properties drwxrwxr-x swivel swivel tmp -rw-rw-r-- swivel swivel verifyKey.dat

/pinsafe/WEB-INF/ -rw-rw-r-- swivel swivel debug.log -rw-rw-r-- swivel swivel pinsafe.log

/pinsafe/WEB-INF/data -rw-rw-r-- swivel swivel repository.xml