Server Administration Guide to Cantr II

Server Administration Team
server@cantr.net

November 5, 2011

Contents

1 Introduction **1**

2 Security and protection **1**
2.1 Intrusion detection system 2

3 Production environment **3**

4 Test environment **3**

5 Game downtime **3**

1 Introduction

This document provides information for server administrators on Cantr III.

Note that some important server scripts and configuration files are stored in the Subversion archive under

`cantr_server/script_archive`

See the programmers manual for further details on how to use Subversion. Please make sure that when changes are made to the server configuration, the script_archive is updated as well.

2 Security and protection

`/etc/ssh/sshd_config`

Last line lists the users that are allowed to use SSH to connect to the server.

comment

Install port knock?

`/etc/cron.deny`

lists users that are not allowed to run cron-jobs.

comment

Should this not be a list of users who are allowed?

2.1 Intrusion detection system

As part of the security system on the server we make use of OSSEC[1], which monitors many log files and provides warning emails if anything suspicious happens. "OSSEC is an Open Source Host-based Intrusion Detection System. It performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response." It also automatically blocks IP addresses on the firewall (/etc/hosts.deny) if it has clear indications of an attack on the server.

The configuration of OSSEC can be found here:

`/var/ossec/etc/ossec.conf`

OSSEC currently monitors:

```
/var/log/messages
/var/log/auth.log
/var/log/syslog
/var/log/mail.info
/var/log/dpkg.log
/var/log/apache2/error.log
/var/log/apache2/access.log
```

comment

What about /home/http/*/*.log?

[1] http://www.ossec.net/

To start OSSEC:

```
/var/ossec/bin/ossec-control start
```

This is also automatically done at a reboot of the server. To stop OSSEC:

```
/var/ossec/bin/ossec-control stop
```

3 Production environment

The production environment is the code on the real game server and the server that runs the clock on the same server. The production code of the web interface is located at:

```
/home/http/www.cantr.net/www/
```

The directory structure is, hopefully, straightforward. All web code is located in the http directory, in the www subdirectory. For the code to be accessible, the web server needs to be running, which can be started with:

```
/etc/init.d/apache start
```

as well as the database server:

```
/etc/init.d/mysql start
```

For the clock to tick in the game, two additional programs have to be started, one for the main game and one for the test environment:

```
nice -n 10 nohup /home/cantr/server &
nice -n 10 nohup /home/cantr/server_test &
```

4 Test environment

5 Game downtime

There are a few simple steps someone must take when the server has to be down for planned maintenance or for other reasons, as long as it is for a long time. If you have direct access (SSH) to the server go to www.cantr.net and:

```
mv index.html.downtime index.html
```

As index.html has precedence over index.php in the apache setting, this will now be the default document of the server. If you want a custom message to be displayed, edit the line "Cantr II is currently not available". Next you have to make a change to index.php. Right after

```
<?php
```

add the line:

```
header('Location: http://cantr.net');
```

This will redirect anyone trying to access the site from a bookmark pointing at, or directly at, http://cantr.net/index.php?lang=.... (or something) to our new default document.

When the site is about to go online again, remove that line from index.php and:

```
mv index.html index.html.downtime
```