Set up the erp Jail: Your ERP Application Server

by Christoph H. Larsen — last modified Nov 08, 2011 08:18 AM Copyright 2010 - TODAY synaLinQ

Contents

Create the Jail

Issue as root from the base system (subsequently called *host*):

```
ezjail-admin create -f common erp 127.0.1.108
```

From within the host, start the jail, which triggers flavourisation:

```
ezjail-admin start erp
```

Edit /usr/local/etc/ezjail/erp on host as follows (only changed sections are shown):

```
# PROVIDE: erp_ezjail
# REQUIRE: mail_ezjail
```

Back to top

Prepare Mount Point and User for Tryton Server

Issue the following as root from the base system to create a non-privileged user for trytond, to create a corresponding mount points and to adjust /etc/fstab:

```
mkdir /home/tryton
pw groupadd tryton -g 2500
pw useradd -c "trytond user" -d /home/tryton -n tryton -s /usr/sbin/nologin -u 2500 -w no
chown root:tryton /home/tryton
chmod 770 /home/tryton
echo "/home/tryton                    /usr/jails/erp/home/tryton                      nullfs  rw,nosuid
```

Now, **enter the jail**, and create a non-privileged user for the zope instance, as well as some essential directories:

```
ezjail-admin console erp
mkdir -p /home/tryton /var/run/trytond
pw groupadd tryton -g 2500
pw useradd -c "trytond user" -d /home/tryton -n tryton -s /bin/csh -u 2500 -w no
chown root:tryton /home/tryton /var/run/trytond
chmod 770 /home/tryton /var/run/trytond
```

Exit to host and mount the instance home directory:

```
exit
mount -a
```

Back to top

Install Midnight Commander

Enter the erp jail and install mc:

```
ezjail-admin console erp
cd /usr/ports/misc/mc-light && make deinstall install distclean
```

Program	System Prompt	Your Response
mc-light	*Enable gettext support*	Yes
	Allow run mc inside mc	Yes
		Note: **Leave all other options deselected!**
libiconv		
		Note: **Leave all options deselected!**

Back to top

Install nullmailer

From within the jail, issue as root:

```
cd /usr/ports/mail/nullmailer && make deinstall install distclean
chown nullmail:wheel /var/spool/nullmailer/*
/usr/local/etc/rc.d/nullmailer restart
```

Note: The configuration of nullmailer has already been completed via the common flavour jail template.

Back to top

Install portaudit

From within the jail, issue as root:

```
cd /usr/ports/ports-mgmt/portaudit && make deinstall install distclean
rehash
```

Create the portaudit database as follows:

```
portaudit -Fda
```

Note: portaudit will automatically install a cron job, and is executed daily.

Back to top

Install portmaster

From within the jail, issue as root:

```
cd /usr/ports/ports-mgmt/portmaster && make deinstall install distclean
```

Note: **Leave all options deselected!**
Note: **If you want to force the install or upgrade of a port with prevalent security warnings, launch portmaster with the "-m DISABLE_VULNERABILITIES=yes" option.**

Back to top

Install Python

From within the jail issue:

```
cd /usr/ports/lang/python27 && make deinstall install distclean
```

System Prompt	Your Response
Enable thread support	Yes
Use UCS24 for unicode support	Yes
Enable python's internal malloc	Yes
***Note:* Leave all other options deselected!**	

Back to top

Install py-libxml

From within the jail issue:

```
cd /usr/ports/devel/py-lxml && make deinstall install distclean
```

System Prompt	Your Response
Enable crypto support for exslt	Yes
***Note:* Leave all other options deselected!**	

Back to top

Install py-relatorio

From within the jail issue:

```
cd /usr/ports/print/py-relatorio && make deinstall install distclean
```

Program	System Prompt	Your Response
py*27*-pycha	*Add support for py-cairo*	Yes
cairo	*Enable XCB support*	Yes
	Enable GObject function feature	Yes
	***Note:* Leave all other options deselected!**	
png		
	***Note:* Leave all options deselected!**	
pixman		

		Note: **Leave all options deselected!**
perl	*Use 64-bit integers*	Yes
	Build threaded perl	Yes
	Use multiplicity	Yes
		Note: **Leave all other options deselected!**
pcre	*Enable just-in-time compiling support*	Yes
		Note: **Leave all other options deselected!**
glib		
		Note: **Leave all options deselected!**
gamin		
		Note: **Leave all options deselected!**
py27-yaml		
		Note: **Leave all options deselected!**

Back to top

Install py-dateutil

From within the jail issue:

```
cd /usr/ports/devel/py-dateutil && make deinstall install distclean
```

Back to top

Install simplejson

From within the jail issue:

```
cd /usr/ports/devel/py-simplejson && make deinstall install distclean
```

Back to top

Install py-psycopg2

From within the jail issue:

```
cd /usr/ports/databases/postgresql91-client && make deinstall install distclean
```

Program	System Prompt	Your Response
postgresql-client	*Use internationalised messages*	Yes
	Builds with compiler optimisations	Yes
	Build with XML data type	Yes
	Use internal timezone database	Yes
	Builds with 64-bit date/time type	Yes
	Build with OpenSSL support	Yes
		Note: **Leave all other options deselected!**

From within the jail issue:

```
cd /usr/ports/databases/py-psycopg2 && make deinstall install distclean
```

Back to top

Install py-pywebdav

From within the jail issue:

```
cd /usr/ports/www/py-pywebdav && make deinstall install distclean
```

Back to top

Install py-pydot

From within the jail issue:

```
cd /usr/ports/graphics/py-pydot && make deinstall install distclean
```

Program	System Prompt	Your Response
graphviz	*Build with ICONV support*	Yes
	Build with XPM support	Yes
	DIGCOLA features in neato layout	Yes
	IPSECOLA features in neato layout	Yes
	Build with gettext support	Yes
	Build with pangocairo support	Yes
		Note: **Leave all other options deselected!**

m4		
		Note: **Leave all options deselected!**
gd	*fontconfig library support*	Yes
	iconv support	Yes
		Note: **Leave all other options deselected!**

Back to top

Install py-pytz

From within the jail issue:

```
cd /usr/ports/devel/py-pytz && make deinstall install distclean
```

Back to top

Install py-sphinx

From within the jail issue:

```
cd /usr/ports/textproc/py-sphinx && make deinstall install distclean
```

Program	System Prompt	Your Response
py27***-Jinja2***	*Enable speedups*	Yes
		Note: **Leave all other options deselected!**

Back to top

Install py-openssl

From within the jail issue:

```
cd /usr/ports/security/py-openssl && make deinstall install distclean
```

Back to top

Install py-ldap2

From within the jail issue:

```
cd /usr/ports/net/py-ldap2 && make deinstall install distclean
```

Program	System Prompt	Your Response
openldap-client	*With (Cyrus) SASL2 support*	Yes
Note: **Leave all other options deselected!**		
cyrus-sasl	*Enable cmusaslsecretCRAM-MD5 property*	Yes
	Enable use of authdaemon	Yes
	Enable LOGIN authentication	Yes
	Enable PLAIN authentication	Yes
	Enable CRAM-MD5 authentication	Yes
	Enable DIGEST-MD5 authentication	Yes
	Enable NTLM authentication	Yes
	Enable SCRAM authentication	Yes
Note: **Leave all other options deselected!**		

Back to top

Install unzip

Issue the following from within the jail:

```
cd /usr/ports/archivers/unzip && make deinstall install distclean
```

Back to top

Install py-pip

Issue the following from within the jail:

```
cd /usr/ports/devel/py-pip && make deinstall install distclean
mkdir -p /usr/local/src
```

Back to top

Install py-polib

Issue the following from within the jail:

```
cd /usr/ports/devel/py-polib && make deinstall install distclean
```

Back to top

Create Local Tryton Server Certificate

Exit to host, and create local server certificate **from within host**:

```
exit
/root/bin/create_jail_certificates erp
```

System Prompt	Your Response
Check for errors, press any key to continue...	[Enter]
Enter pass phrase for /etc/ssl/private/ca.lims.mri.gov.lk.cakey.pem:	[CA key pass phrase]
Sign the certificate?	y
1 out of 1 certificate requests certified, commit?	y
Check for errors, press any key to continue...	[Enter]
***Note:* This will also copy the local server key and certificate into the correct locations inside the jail.**	

Enter the erp jail, and add the tryton user to the ssl-cert group to enable access to the pgsql private key and bundle:

```
ezjail-admin console erp
pw groupmod ssl-cert -m tryton
```

From with the jail, adjust permissions:

```
setenv DOMAIN erp.jail.vlan
chown root:ssl-cert /etc/ssl/private/${DOMAIN}.key.pem /etc/ssl/private/${DOMAIN}.key+crt.pem
chmod 440 /etc/ssl/private/${DOMAIN}.key.pem /etc/ssl/private/${DOMAIN}.key+crt.pem
```

Back to top

Install the Tryton server (trytond)

From within the jail issue:

```
pip install --build-dir=/usr/local/src trytond
pip install --build-dir /usr/local/src trytond_account
pip install --build-dir /usr/local/src trytond_account_be
pip install --build-dir /usr/local/src trytond_account_de_skr03
pip install --build-dir /usr/local/src trytond_account_invoice
pip install --build-dir /usr/local/src trytond_account_invoice_history
pip install --build-dir /usr/local/src trytond_account_invoice_line_standalone
pip install --build-dir /usr/local/src trytond_account_product
pip install --build-dir /usr/local/src trytond_account_statement
pip install --build-dir /usr/local/src trytond_account_stock_anglo_saxon
pip install --build-dir /usr/local/src trytond_account_stock_continental
pip install --build-dir /usr/local/src trytond_analytic_account
pip install --build-dir /usr/local/src trytond_analytic_invoice
pip install --build-dir /usr/local/src trytond_analytic_purchase
pip install --build-dir /usr/local/src trytond_analytic_sale
```

```
pip install --build-dir /usr/local/src trytond_calendar
pip install --build-dir /usr/local/src trytond_calendar_classification
pip install --build-dir /usr/local/src trytond_calendar_scheduling
pip install --build-dir /usr/local/src trytond_calendar_todo
pip install --build-dir /usr/local/src trytond_carrier
pip install --build-dir /usr/local/src trytond_company
pip install --build-dir /usr/local/src trytond_company_work_time
pip install --build-dir /usr/local/src trytond_country
pip install --build-dir /usr/local/src trytond_currency
pip install --build-dir /usr/local/src trytond_dashboard
pip install --build-dir /usr/local/src trytond_google_maps
pip install --build-dir /usr/local/src trytond_ldap_authentication
pip install --build-dir /usr/local/src trytond_ldap_connection
pip install --build-dir /usr/local/src trytond_party
pip install --build-dir /usr/local/src trytond_party_siret
pip install --build-dir /usr/local/src trytond_party_vcarddav
pip install --build-dir /usr/local/src trytond_product
pip install --build-dir /usr/local/src trytond_product_cost_fifo
pip install --build-dir /usr/local/src trytond_product_cost_history
pip install --build-dir /usr/local/src trytond_product_price_list
pip install --build-dir /usr/local/src trytond_project
pip install --build-dir /usr/local/src trytond_project_plan
pip install --build-dir /usr/local/src trytond_project_revenue
pip install --build-dir /usr/local/src trytond_purchase
pip install --build-dir /usr/local/src trytond_purchase_invoice_line_standalone
pip install --build-dir /usr/local/src trytond_sale
pip install --build-dir /usr/local/src trytond_sale_opportunity
pip install --build-dir /usr/local/src trytond_sale_price_list
pip install --build-dir /usr/local/src trytond_sale_shipment_cost
pip install --build-dir /usr/local/src trytond_stock
pip install --build-dir /usr/local/src trytond_stock_forecast
pip install --build-dir /usr/local/src trytond_stock_inventory_location
pip install --build-dir /usr/local/src trytond_stock_location_sequence
pip install --build-dir /usr/local/src trytond_stock_product_location
pip install --build-dir /usr/local/src trytond_stock_supply
pip install --build-dir /usr/local/src trytond_stock_supply_day
pip install --build-dir /usr/local/src trytond_stock_supply_forecast
pip install --build-dir /usr/local/src trytond_timesheet
pip install --build-dir /usr/local/src trytond_health_profile
```

Back to top

Configure trytond

You need the trytond configuration file that corresponds to the version you are going to use, so get it as follows from within the jail.
⚠ Make sure you adjust TRYTOND_VERSION to the correct version in current use!

```
set TRYTOND_VERSION=2.2.0
mkdir -p /root/packages/tryton
cd /root/packages/tryton
fetch http://downloads.tryton.org/current/trytond-${TRYTOND_VERSION}.tar.gz
tar xzf ./trytond-${TRYTOND_VERSION}.tar.gz
cp -f /root/packages/tryton/trytond-${TRYTOND_VERSION}/etc/trytond.conf /usr/local/etc/trytond.conf
rm -rf ./trytond-${TRYTOND_VERSION}/
chown -R root:wheel /root
chmod -R 600 /root
chmod u+X /root
chmod -R 700 /root/bin
unset TRYTON_VERSION
```

From within the jail, backup the original configuration file as follows:

```
cp /usr/local/etc/trytond.conf /usr/local/etc/trytond.conf.orig
```

From with the jail, edit /usr/local/etc/trytond.conf as follows (only changed sections are shown):

```
#hostname =
hostname = erp.synalinq.net

#jsonrpc = localhost:8000
jsonrpc = 127.0.1.108:8000
#ssl_jsonrpc = False
ssl_jsnorpc = True

#jsondata_path = /var/www/localhost/tryton
jsondata+path = /home/tryton/jsondata

#webdav = *:8080
webdav = 127.0.1.108:8080
#ssl_webdav = False
ssl_webdav = True

#db_host = False
db_host = 127.0.1.104
#db_port = False
db_port = 5432
#db_user = False
db_user = tryton
#db_password = False
db_password = [db_user password]

#admin_passwd = admin
admin_passwd = [admin password]

#pidfile = False
pidfile = /var/run/trytond/trytond.pid
#logfie = False
logfile = /var/log/trytond/trytond.log

#privatekey = server.pem
privatekey = /etc/ssl/private/erp.jail.vlan.key.pem
#certificate = server.pem
certificate = /etc/ssl/certs/erp.jail.vlan.crt.pem

#smtp_server = localhost
smtp_server = mail.jail.vlan

#data_path = /var/lib/trytond
data_path = /home/tryton/data
```

From within the jail, create directories for pidfile and logs, and adjust permissions:

```
chown root:tryton /usr/local/etc/trytond.conf*
chmod 640 /usr/local/etc/trytond.conf*
mkdir -p /var/log/trytond /var/run/trytond
chown root:tryton /var/log/trytond /var/run/trytond
chmod 770 /var/log/trytond /var/run/trytond
mkdir -p /home/tryton/data /home/tryton/jsondata
chown -R root:tryton /home/tryton
chmod -R 660 /home/tryton
chmod -R ug+X /home/tryton
```

From inside the jail, issue the following to have log rotation effected for each instance of zope:

```
echo '/var/log/trytond/trytond.log  root:tryton  660  7  *    $D0   GJ' >> /etc/newsyslog.conf
```

From within the jail, create /usr/local/etc/rc.d/trytond as follows:

```
#!/bin/sh
```

```
#
# PROVIDE: trytond
# REQUIRE: DAEMON
# BEFORE:  LOGIN

. /etc/rc.subr

name=trytond
rcvar=`set_rcvar`

load_rc_config $name

: ${trytond_enable="NO"}
: ${trytond_user="tryton"}
: ${trytond_group="tryton"}

start_cmd=${name}_start
stop_cmd=${name}_stop
restart_cmd=${name}_restart
status_cmd=${name}_status

command="/usr/local/bin/trytond"
required_files="/usr/local/etc/trytond.conf"

trytond_start() {
 su tryton -c "$command --config=/usr/local/etc/trytond.conf" &
}

trytond_stop() {
    if [ -f /var/run/${name}/${name}.pid ]; then
        kill `cat /var/run/${name}/${name}.pid`
    fi
}

trytond_restart() {
    if [ -f /var/run/${name}/${name}.pid ]; then
        kill `cat /var/run/${name}/${name}.pid`
        sleep 1
    fi
    su tryton -c "$command --config=/usr/local/etc/trytond.conf" &
}

run_rc_command "$1"
```

From within the jail, adjust permissions:

```
chown root:wheel /usr/local/etc/rc.d/trytond
chmod 755 /usr/local/etc/rc.d/trytond
```

From within the jail, issue the following to autostart trytond:

```
echo '' >> /etc/rc.conf
echo '# Enable trytond' >> /etc/rc.conf
echo 'trytond_enable="YES"' >> /etc/rc.conf
```

Exit to host and enter the pgsql jail, and create the datbase user tryton:

```
cd /tmp
su pgsql
csh
createuser --createdb --no-createrole --no-superuser --pwprompt tryton
```

System Prompt	Your Response

Enter password for new role:	[tryton password]
Enter it again:	[tryton password]

Exit to host and issue as root:

```
ezjail-admin restart pgsql erp
```

Back to top

Install the Tryton Client (tryton):

On your local workstation, install Python (recommended version 2.7), and python-pip. Thereafter, issue:

```
pip install tryton
```

Back to top

Perform Post-Installation Configuration for Tryton:

On your local workstation, start the Tryton client, and set the Tabs position to top:

Go to	Your Response
Options	
Form	
Tab positions	Top
Options	
Email	/bin/echo '${body}' | /usr/bin/uuencode ${attachment} \| /usr/bin/mail -s '${subject}' -c ${cc} ${to}

Back to top

Install the OSSEC Agent

From within the jail, issue:

```
set OSSEC_VERSION=2.6
mkdir -p /root/packages/ossec
cd /root/packages/ossec
fetch http://www.ossec.net/files/ossec-hids-${OSSEC_VERSION}.tar.gz
chown -R root:wheel /root
chmod -R 600 /root
```

```
chmod -R u+X /root
chmod -R 700 /root/bin
tar xzf /root/packages/ossec/ossec-hids-${OSSEC_VERSION}.tar.gz
cd ossec-hids-${OSSEC_VERSION}
cd src; make setdb; cd ..
./install.sh
```

System Prompt	Your Response
For installation in English, choose [en]:	en
What kind of installation do you want?	agent
Choose, where to install OSSEC HIDS:	/usr/local/ossec
What is the IP address of the OSSEC HIDS server?	127.0.1.254
Do you want to run the integrity check daemon?	y
Do you want to run the rootkit detection engine?	y
Do you want to enable active response?	y
***Note:* In the case of deinstallation, you have to delete /usr/local/ossec manually.**	

From with the jail, clean up and make configuration files more accessible:

```
cd /
rm -rf /root/packages/ossec/ossec-hids-${OSSEC_VERSION}
cp /usr/local/ossec/etc/ossec.conf /usr/local/ossec/etc/ossec.conf.orig
ln -fs /usr/local/ossec/etc/ossec.conf.orig /usr/local/etc/ossec.conf.orig
ln -fs /usr/local/ossec/etc/ossec.conf /usr/local/etc/ossec.conf
```

Edit /usr/local/ossec/etc/ossec.conf as follows (only changed sections are shown):

```
    <!-- Directories to check  (perform all possible verifications) -->
    <directories check_all="yes">/etc</directories>
    <directories check_all="yes">/usr/local/bin,/usr/local/sbin</directories>
    <directories check_all="yes">/root/bin</directories>
```

Note: /bin, /sbin, /usr/bin and /usr/sbin are just links to the respective host's directories, and therefore not monitored from within the jails.

Open another terminal window, log into the server via SSH, and issue the following **from inside host**:

```
/usr/local/ossec/bin/manage_agents
```

System Prompt	Your Response
Choose your action:	e
Provide the ID of the agent to extract the key:	108

Note: **Keep this terminal window open and copy the key issued onto your workstation's clipboard!**	
	[Enter]
Choose an action:	q

From the previous terminal window, issue **inside the jail**:

```
/usr/local/ossec/bin/manage_agents
```

System Prompt	**Your Response**
Choose your action:	i
Note: **Paste the key issued by the OSSEC server here!**	
Confirm adding:	y
	[Enter]
Choose an action:	q

From within the jail, issue:

```
/usr/local/etc/rc.d/ossec-hids restart
```

Exit to host, and issue:

```
exit
/usr/local/etc/rc.d/ossec-hids restart
```

Test the OSSEC system from within the host. First, collect the server data by issuing:

```
/usr/local/ossec/bin/agent_control -i 000
```

Now, collect data from the lims jail:

```
/usr/local/ossec/bin/agent_control -i 108
```

Note: You should see up-to-date agent information for the server (ID: 000) and the erp jail (ID: 108), stating:
Status: Active

Back to top

Clean up

As each newly installed program is compiled, which in turn uses a few auxiliary programs, it is necessary to clean up after each compilation. From within the jail, issue:

```
cd /var/db/pkg
portmaster -l
```

Note: Identify non-required programs in the "Root ports" and "Leaf ports" categories, only. Then, issue as root:

```
pkg_delete [name of program to be deleted][tab]
```

Note: Repeat as required, for "Root ports" and "Leaf ports", *only*.
*Noite:*Likely candidates for removal are: bdftopcf*, bigreqsproto*, bison*, gmake*, gperf*, inputproto*, libcheck*, libtool*, xcb-proto*, xcmiscproto*, xf86bigfontproto*, xorg-macros*, xtrans* .
Now, deploy portmaster's automatic clean-up mechanisms from within the jail to deal with the rest:

```
portmaster -s
portmaster -y --clean-distfiles
portmaster --check-depends
portmaster --check-port-dbdir
```

Note: Reply "y" as prompted, to have all dependent packages purged.

Back to top

- 

Add comment

You can add a comment by filling out the form below. Plain text formatting. Web and email addresses are transformed into clickable links.

Comment ■

Notify me of new comments via email.