

Network Services

Disaster Recovery

This is the documentation for the infrastructure at Martin Luther College. The idea is to document everything well-enough that a person would be able to know what is where and what it does to get things back up-and-running.

We will also hold information for some known issues when bringing servers up from being powered-off.

- [Servers](#)
- [Server Incantations](#)
- [Upgrading SLE](#)
- [Mapped Drives Not Available in Windows Save Dialogs](#)
- [Creating Library Student Worker Accounts](#)
- [Superfluous eDirectory Accounts](#)
- [DRBD Recovery](#)
- [Tegile Array Information](#)
- [CWDB](#)
- [CWDB Archive](#)
- [CWDB Backup](#)
- [Backup Process](#)
- [WordPress Customizations](#)
- [DMZ Hosts & IP Addresses](#)
- [SSL Certificates](#)
- [Orbeon Setup](#)
- [Daily Ops Duties](#)
- [XenServer Cluster Documentation](#)
- [XenServer Recovery and Other Things](#)

- [Xen Appliance Conversion](#)
- [CWDB Dev Server Refresh Scripts](#)
- [FreePBX](#)
- [Comcast Documentation and Information](#)
- [Updating the Call List on Call Day](#)
- [Moodle](#)
- [Student Worker Admin Accounts](#)
- [Network Services Admin Accounts](#)
- [Trane Cloud VPN](#)
- [Goats](#)

Servers

- [Incantations](#)
- [Upgrading SLE](#)

Physical

| Name | DNS | IP Address | Loc | OS | Ver | Services |
|----------------------------|------------|--------------|----------|----------|------|----------------------|
| Portal | portal | 172.16.1.131 | | RHEL | 5.10 | portal, imsexport |
| Reggie | reggie | 172.16.0.2 | | RHEL | 5.10 | reggie |
| Panda | panda | 172.16.0.1 | | RHEL | 4 | panda |
| Zoneminder | zoneminder | 172.16.0.52 | NS01:C22 | CentOS | 7 | zoneminder |
| Backup | backup | 172.16.0.47 | | openSUSE | 42.1 | bareos |

Internal XenServer Cluster

Hosts

| Name | DNS | IP Address | Loc | OS | Ver | Services |
|--------|------|--------------|-----|-----------|-----|-----------|
| Zerah | null | 172.16.0.135 | | XenServer | 6.2 | xenserver |
| Pharez | null | 172.16.0.134 | | XenServer | 6.2 | xenserver |

Virtual Machines

| Name | DNS | IP Address | OS | Ver | Services |
|--------------|--------------|--------------|-----------|-----------|-------------|
| Bond | null | 172.17.0.7 | Ubuntu | 12.04 | bind |
| BondSlave | null | 172.17.0.9 | Ubuntu | 12.04 | bind |
| CWDB | cwdb | 172.16.1.128 | SLES | 12 | postgresql |
| CWDB Archive | cwdb-archive | 172.16.1.129 | SLES | 12 | null |
| iPrint | iprint | 172.16.1.17 | Appliance | | iprint |
| Pioneer | null | 172.16.4.42 | Windows | 7 | iMAP |
| Cacti | cacti | 172.16.0.53 | Ubuntu | 14.04 | cacti |
| PaperCut | papercut | 172.16.1.15 | SLES | 11 SP3 | papercut |
| SchaeffM | null | 172.16.1.94 | Windows | 7 | rdp, access |
| StarrRD | null | 172.16.1.92 | Windows | 7 | rdp, access |
| Support | support | 172.16.0.61 | Ubuntu | 12.04 | rt |
| UniFi | unifi | 172.16.0.65 | Ubuntu | 14.04 | unifi |
| UnkeLL | null | 172.16.1.90 | Windows | 7 | rdp, access |
| XOA | orchestra | 172.16.0.63 | XOA | Appliance | orchestra |

Access Virtual Machines

| Name | DNS | IP Address | OS | Ver | Services |
|----------|------|-------------|---------|-----|-------------|
| StarrAM | null | 172.16.1.95 | Windows | 10 | rdp, access |
| RiderEG | null | 172.16.1.91 | Windows | 10 | rdp, access |
| StarrRD | null | 172.16.1.92 | Windows | 10 | rdp, access |
| UnkeLL | null | 172.16.1.90 | Windows | 10 | rdp, access |
| BiedenDK | null | 172.16.1.93 | Windows | 10 | rdp, access |
| SchaeffM | null | 172.16.1.94 | Windows | 10 | rdp, access |

External XenServer Cluster

Hosts

| Name | DNS | IP Address | Loc | OS | Ver | Services |
|---------|------|----------------|-----|-----------|-----|-----------|
| Apollo | null | 192.168.95.201 | | XenServer | 6.2 | xenserver |
| Artemis | null | 192.168.95.200 | | XenServer | 6.2 | xenserver |

Virtual Machines

| Name | DNS | IP Address | OS | Ver | Services |
|-----------------------|-------------|----------------|-----------|--------|-------------|
| NS1 | ns1 | 192.168.95.100 | Ubuntu | 12.04 | bind |
| NS2 | ns2 | 192.168.95.101 | Ubuntu | 12.04 | bind |
| Website | null | 192.168.95.34 | Ubuntu | 12.04 | plone |
| Utility | kb | 192.168.95.13 | SLES | 11 SP3 | dokuwiki |
| Postgres | dmzpostgres | 192.168.95.37 | SLES | 11 SP3 | postgresql |
| MySQL | dmzmysql | 192.168.95.38 | SLES | 11 SP3 | mysql |
| Blogs | blogs | 192.168.95.11 | SLES | 11 SP3 | wordpress |
| Emil | emil | 192.168.95.12 | CentOS | 6.5 | ezproxy |
| NetPartner | aid | 192.168.95.17 | Windows | 2008 | net partner |
| Booked | booked | 192.168.95.22 | SLES | 11 SP3 | booked |
| MLC Moodle | moodle | 192.168.95.6 | SLES | 11 SP3 | moodle |
| ALHSO Moodle | alhso | 192.168.95.18 | SLES | 11 SP3 | moodle |
| Orbeon | orbeon | 192.168.95.41 | SLES | 11 SP3 | orbeon |
| Ralph | ralph | 192.168.95.36 | Ubuntu | 12.04 | ldap |
| Auth | auth | 192.168.94.21 | SLES | 12 | cas, sspr |
| Filr | filr | 192.168.95.19 | Appliance | | filr |

Other

| Name | DNS | IP Address | Loc | OS | Ver | Services |
|------|-----|------------|-----|----|-----|----------|
|------|-----|------------|-----|----|-----|----------|

| | | | | | | |
|--------|--------|--------------|--|------|------|----------------------|
| Portal | portal | 172.16.1.131 | | RHEL | 5.10 | portal, imsexport |
|--------|--------|--------------|--|------|------|----------------------|

Server Incantations

SLES

- `chkconfig -add [service]` - starts the service on startup
- `rpm -i [path to installation rpm]` - installs the rpm (useful for installing xs-tools on a host not included in the `install.sh` file)
- `zypper up` - upgrade server to latest package revisions
- `zypper search` - search for packages containing the term you want
- `zypper dup --no-allow-vendor-change` - safer way to upgrade servers with additional repos
- `rc[process name] start|stop|restart|reload` - manage processes (tab will show you the available processes)
- `SuSEfirewall2` - load and apply any custom firewall rules you have setup within YaST

Upgrading SLE

From SLE 11 SP3 to SLE 11 SP4

Taken from <https://www.suse.com/support/kb/doc.php?id=7016711>.

- `zypper ref -s`
- `zypper update -t patch`
- `zypper update -t patch` (again)
- `zypper se -t product | grep -h - "-migration" | cut -d\| -f2`
- A sample output could be as follows: `SUSE_SLES-SP4-migration`
- `zypper in -t product sle-sdk-SP4-migration SUSE_SLES-SP4-migration` (modify from what is shown in above command)
- `suse_register -d 2 -L /root/.suse_register.log`
- `zypper ref -s`
- `zypper lr`
- `zypper mr --disable <repo-alias>` any repos that are not needed
- `zypper dup --from SLES11-SP4-Pool --from SLES11-SP4-Updates` plus other repos as needed
- `suse_register -d 2 -L /root/.suse_register.log`
- Reboot the machine

From SLE 12 to SLE 12 SP1

Taken from https://www.suse.com/documentation/sles-12/book_sle_deployment/data/sec_update_migr_zypper_onlinemigr.html.

- Install the latest updates.
- Install the packages `zypper-migration-plugin` and their dependencies.
- Run the zypper migration: `zypper migration`.
- Review all the changes, especially the packages that are going to be removed. Proceed by typing y.
- After successful migration restart your system.

Slow Boot Issues after Service Pack Migration

Check the boot loader in YaST for incorrect drive names both for the boot device and the kernel parameters.

Mapped Drives Not Available in Windows Save Dialogs

- <https://www.novell.com/support/kb/doc.php?id=7009906>
- <https://social.technet.microsoft.com/Forums/en-US/62456d84-95a1-4d43-9745-d8c4e8e600fb/since-kb3194798-enablelinkedconnections-is-not-working-anymore-mapping-shares-mmc-on-network?forum=win10itprogeneral>

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\ EnableLinkedConnections =1
```

```
New-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -PropertyType DW
```

Creating Library Student Worker Accounts

1. Select an unassigned WorkerXX.wrk.lib.ac.mlc account to assign
2. Configure WorkerXX with appropriate group memberships
3. Configure WorkerXX with additional permissions as appropriate
4. Be sure to configure station access restrictions as necessary
5. Create an alias object in staff.lib.ac.mlc with the student's login name
6. Set a temporary password on WorkerXX
7. Student logs in using the distinguished name of the alias object (e.g. *spikeac.staff.lib.ac.mlc*) and the temporary password assigned for WorkerXX

Current Active Worker Accounts

| Username | Alias |
|----------|----------|
| worker01 | nguyenmt |
| worker02 | kohlssa |
| worker03 | |
| worker04 | |
| worker05 | |

Superfluous eDirectory Accounts

These are current accounts which are not in the database as of 2017-01-16.

```
['wilsonbk', 'wagneras', 'penterwl', 'malkowjt', 'henselrh', 'buchhomd', 'townewm', 'schmitan', 'schlotkr', 'rynohg',  
'retberan', 'nusharsm', 'millerrh', 'lochharc', 'lindemmr', 'has', 'everslj', 'bramstar', 'boveeke', 'andersre', 'walkerlm',  
'miskotc', 'barretse', 'wileyca', 'weinstae', 'wallaj', 'viethsnj', 'tenyerjl', 'swansose', 'stuevecb', 'stanosta', 'schumass',  
'schliemd', 'richardj', 'pretzear', 'polferrj', 'lindowkc', 'lincejm', 'kinneyee', 'kietahm', 'hollinca', 'hartmacj', 'greenwmp',  
'franckag', 'douglarw', 'davisec', 'boylansm', 'bowlesmr', 'borreeka', 'krauseba', 'danelljm']
```

DRBD Recovery

This is documentation to bring back the old (Ubuntu 12.04) storage servers from a cold start to being able to connect with the XenServer cluster over NFS.

Current Configuration

Internal

- Esau - primary/nfs
- Jacob - secondary

External

- Remus - primary/nfs
- Romulus - secondary

The Steps

- bring servers back from the dead, you can have them both up before starting anything
- `modprobe drbd` - checks and enables the proper kernel module
- `drbd-overview` - check `drbd` status
- On Primary
 - `drbdadm connect [i]nfs[1/2]` - connect to the `drbd` shares
- On Secondary
 - `drbdadm - -discard-my-data connect [i]nfs[1/2]` - connect to the `drbd` shares
- On Primary
 - `drbdadm primary [i]nfs[1/2]` - set the primary server as the primary device within `drbd`
 - `mount -o noatime /dev/drbd0 /srv/[i]nfs[1/2]` - mount the `drbd` block device to the proper mount point
 - `service nfs-kernel-service start` - start the `nfs` service

You can now have the XenServer cluster go ahead and fix the NFS SR issues. Things should now be working.

Tegile Array Information

Networking Information

- SMTP: mailhost.mlc-wels.edu
- Email: servers@mlc-wels.edu
- NTP: 0.pool.ntp.org
- DNS: 192.168.95.100 192.168.95.101
- DNS Suffix: mlc-wels.edu

T3100 - Jacob

- Location: WCC Primary Server Room

Switch Ports

NS01

- Unordered List Item

iSCSI VLAN

- 192.168.91.10 - Floating IP
- 192.168.91.11 - Jacob-A
- 192.168.91.12 - Jacob-B
- 192.168.91.13 - -Floating IP

Management VLAN

- 172.16.0.200 - Array Floating IP
- 172.16.0.201 - Jacob-A IP
- 172.16.0.202 - Jacob-B IP
- 172.16.0.203 - Jacob-A IPMI

- 172.16.0.204 - Jacob-B IPMI

SS2100 - Esau (Offline)

- Location: Chapel of the Christ Secondary Server Room

Switch Ports

CC01

- Unordered List Item

iSCSI VLAN

- 192.168.91.14
- 192.168.91.15

Management VLAN

- 172.16.0.205 - Controller IP
- 172.16.0.206 - IMPI

HA2100 - Isaac (Temp)

- Location: Chapel of the Christ Secondary Server Room

Switch Ports

- Unordered List Item

iSCSI VLAN

- 192.168.91.14

Academic VLAN

- 172.16.0.210 - Controller Management
- 172.16.0.211
- 172.16.0.212
- 172.16.0.213
- 172.16.0.214

CWDB

| DNS | IP Address | Loc | OS | Ver | Services |
|------|--------------|-------------|------|-----|------------|
| cwdb | 172.16.1.128 | Internal VM | SLES | 12 | postgresql |

Installation

SLE Modules

- Software Development Kit
- Web and Scripting

Installed Packages

- postgresql

Users

- postgres (created when installing the postgresql package)

Useful Incantations

Managing PostgreSQL Process

```
rcpostgresql start|stop|restart|reload
```

Load Firewall Rules

```
SuSEfirewall2
```

Cron Jobs

Root

Copies custom firewall rules into area where normal backups can grab a copy and changes the ownership so that it can be copied over easily.

```
0 0 * * * cp bin/SuSEfirewall2-custom /var/lib/pgsql/data/ | chown postgres:postgres /var/lib/pgsql/data/SuSEfirewal
```

Postgres

Runs the backup script that copies the `/data` directory via `rsync`.

```
15 3 * * * /var/lib/pgsql/bin/pg_binary_backup.sh >/dev/null 2>&1
```

Firewall

There is a need for custom rules for the firewall to handle PostgreSQL and SSH connections. They are stored in `/root/bin/SuSEfirewall2-custom`. You can find a copy of this file within the binary backup of the `/data` directory for cwdb stored on archive.

- You will need to tell SUSE to load these custom rules by going to `YaST > System > /etc/sysconfig Editor > Network > Firewall > SuSEfirewall2 > FW_CUSTOMRULES` and then adding `/root/bin/SuSEfirewall2-custom` into the settings
- When you make changes to the custom rules, you will need to run the `SuSEfirewall2` command as `root` (pay attention to any error messages)

Custom Rules File

Add the rules within the `fw_custom_before_masq()` area

SuSEfirewall2-custom

```
# list each host IP address on a new line
SSH_HOSTS="
172.16.0.1
"

for SSH_HOST in $SSH_HOSTS; do
iptables -A input_ext -p tcp -s $SSH_HOST --dport 22 -j ACCEPT
done

# list each host IP address on a new line
PG_HOSTS="
172.16.0.1
"

for PG_HOST in $PG_HOSTS; do
iptables -A input_ext -p tcp -s $PG_HOST --dport 5432 -j ACCEPT
done
```

Backup

WAL archives and `/data` directory backups are housed on the [archive](#) server.

pg_binary_backup.sh

```
#!/bin/bash

CURRENT_DATE=$(date +%y-%m-%d)
DATA_PATH=/var/lib/pgsql/data/
ARCHIVE_DATA_PATH=/home/archive/cwdb/data/$CURRENT_DATE

psql -c "select pg_start_backup('backup for $CURRENT_DATE')"
rsync -cva --inplace --exclude=*pg_xlog* $DATA_PATH archive@172.16.1.130:$ARCHIVE_DATA_PATH
psql -c "select pg_stop_backup(), current_timestamp"
```

CWDB Archive

| DNS | IP Address | Loc | OS | Ver | Services |
|--------------|--------------|-------------|------|-----|----------|
| cwdb-archive | 172.16.1.129 | Internal VM | SLES | 12 | null |

Installation

SLE Modules

- Software Development Kit
- Web and Scripting

Users

- archive

Cron Jobs

Archive

Runs the cleanup script for old backups. Currently only keeping a weeks worth of backups (including WAL archives).

```
15 4 * * * /home/archive/bin/clean_old_backups.sh >/dev/null 2>&1
```

CWDB Backups

Locations

- `/home/archive/cwdb` is the main directory
- `/home/archive/cwdb/wal` directory holds the WAL archives
- `/home/archive/cwdb/data` has a dated directory for each date a full binary backup has been done

Backup Pruning

Currently we keep only a week of backups. This script is run every night and delete the oldest backup.

[clean_old_backups.sh](#)

```
#!/bin/bash

DATA_BACKUP_DIR=/home/archive/cwdb/data/*
WAL_ARCHIVE_DIR=/home/archive/cwdb/wal/*

find /home/archive/cwdb/data/* -maxdepth 0 -type d -mtime +6 -exec rm -rf {} \;
find /home/archive/cwdb/wal/* -maxdepth 0 -mtime +6 -delete
```

CWDB Backup

Backup Overview

The backups for the CWDB are some of the most complex we do on campus. The effect is to allow us to both restore from nothing while losing as few database transactions as possible, and to be able to use PITR (point-in-time recovery) to recover from smaller issues than a complete loss. This is accomplished in three ways:

1. **WAL Archiving** ships the PostgreSQL write-ahead logs to the archive server where they can be “played back” in the future to a certain point-in-time.
2. **Binary Backups** use `rsync` to take complete backups of the entire database `data` directory which allows us to grab not just the data (most important) but also the configuration files for PostgreSQL.
3. Periodically, snapshots of both the binary backup and the wal archives will be committed to tape (or some other off-campus backup solution) for ultimate data recovery options.
This is not yet automated.

That is the 10,000 foot view of what is going on with CWDB backups.

WAL Archiving

Binary Backups

Disaster Recovery Backups

Backup Process

This document lays out how backups are handled.

Cadence

Weekly

- Each Thursday replace the prior longterm archival tape with a different tape for the coming week's archive operation
- Label tape with the date of the archival process (the coming Wednesday)
- IF A USED TAPE clear it before labeling in Bareos with `mt -f /dev/st0 rewind && mt -f /dev/st0 weof && mt -f /dev/st0 rewind` command
- Label the tape using the name `Longterm-YYYY-MM-DD` which matches the label on the outside
- Make sure the naming and mounting processes are successful
- Take the prior archival tape and get it to director for storage offsite

Monthly

- Keep the prior month's latest archival tape for future restores
- Put other tapes into the rotation to be reused for future jobs

Restore Testing

Keep track of when restores and tested, how, and the outcome.

| Date | Restored | Outcome | Who |
|------|----------|---------|-----|
| | | | |

WordPress Customizations

Left Subnavigation Menu

```
.sidebar_left .widget_nav_menu {  
    text-align: left;  
}  
#top .sidebar_left .widget_nav_menu ul ul li:before {  
    left: 1px;  
}
```


DMZ Hosts & IP Addresses

External Hosts

| Server | DMZ Domain | DMZ IP | External Domain | External IP |
|-------------|------------------|---------------|------------------|--------------|
| wwwproxy | wwwproxy | 192.168.95.3 | www | 50.204.85.33 |
| apply | apply | 192.168.95.4 | apply | 50.204.85.34 |
| portalproxy | portalproxy | 192.168.95.5 | portal | 50.204.85.35 |
| moodle | moodle | 192.168.95.6 | moodle | 50.204.85.36 |
| cbemoodle | cbemoodle | 192.168.95.7 | moodle | 50.204.85.37 |
| sspr | sspr | 192.168.95.8 | sspr | 50.204.85.38 |
| admissions | admissions | 192.168.95.9 | admissions | 50.204.85.39 |
| rt | rt | 192.168.95.10 | rt | 50.204.85.40 |
| utility | various | 192.168.95.11 | various | 50.204.85.41 |
| emil | emil | 192.168.95.12 | emil | 50.204.85.42 |
| | | 192.168.95.13 | | 50.204.85.43 |
| cas | cas | 192.168.95.14 | cas | 50.204.85.44 |
| bbb | bbb | 192.168.95.15 | bbb | 50.204.85.45 |
| vpn | vpn | 192.168.95.16 | vpn | 50.204.85.46 |
| netpartner | aid | 192.168.95.17 | aid | 50.204.85.47 |
| alhso | moodle.alhso.org | 192.168.95.18 | moodle.alhso.org | 50.204.85.48 |
| filr | filr | 192.168.95.19 | filr | 50.204.85.49 |
| | | 192.168.95.20 | | 50.204.85.50 |
| auth | auth | 192.168.95.21 | auth | 50.204.85.51 |
| booked | booked | 192.168.95.22 | booked | 50.204.85.52 |
| beta | beta | 192.168.95.23 | beta | 50.204.85.53 |
| vibe | vibe | 192.168.95.24 | vibe | 50.204.85.54 |
| orbeon | orbeon | 192.168.95.25 | orbeon | 50.204.85.55 |

| Server | DMZ Domain | DMZ IP | External Domain | External IP |
|---------------------|------------|---------------|-----------------|--------------|
| meetmath | meetmath | 192.168.95.26 | meetmath | 50.204.85.56 |
| chat | chat | 192.168.95.27 | rocket.chat | 50.204.85.57 |
| login | login | 192.168.95.28 | simplesamlphp | 50.204.85.58 |
| helpdesk | helpdesk | 192.168.95.29 | zammad | 50.204.85.59 |
| orbeon-dev-20200115 | orbeon | 192.168.95.30 | orbeon | 50.204.85.60 |
| netpartner | aid | 192.168.95.31 | aid | 50.204.85.61 |
| | | 192.168.95.32 | | 50.204.85.62 |

Internal Hosts

| Server | DMZ Domain | DMZ IP |
|----------------|----------------|---------------|
| iprint | iprint | 192.168.95.33 |
| website | | 192.168.95.34 |
| backup | backup | 192.168.95.35 |
| ralph | ralph | 192.168.95.36 |
| postgres | dmzpostgres | 192.168.95.37 |
| mysql | dmzmysql | 192.168.95.38 |
| moodle25 | moodle25 | 192.168.95.39 |
| jasper | jasper | 192.168.95.40 |
| dmzpostgresnew | dmzpostgresnew | 192.168.95.41 |
| git | git | 192.168.95.42 |
| mailhost | mailhost | 192.168.95.43 |
| oldlogin | oldlogin | 192.168.95.44 |
| orbeon-test | | 192.168.95.45 |
| wwwproxy | | 192.168.95.46 |
| newapply | newapply | 192.168.95.47 |
| newforms | newforms | 192.168.95.48 |
| mallcam | mallcam | 192.168.95.50 |
| pondcam | pondcam | 192.168.95.51 |
| chapelcam | chapelcam | 192.168.95.52 |

| Server | DMZ Domain | DMZ IP |
|----------------|----------------|----------------|
| moodlecas | moodlecas | 192.168.95.53 |
| | | 192.168.95.54 |
| orbeon-dev | orbeon-dev | 192.168.95.60 |
| cas1 | cas | 192.168.95.70 |
| cas2 | cas | 192.168.95.71 |
| utility | misc | 192.168.95.72 |
| new dmzmysql | mariadb | 192.168.95.73 |
| makerbot | makerbot | 192.168.95.80 |
| ns1 | ns1 | 192.168.95.100 |
| ns2 | ns2 | 192.168.95.101 |
| dns1 | dns1 | 192.168.95.102 |
| dns2 | dns2 | 192.168.95.103 |
| admissions-dev | admissions-dev | 192.168.95.110 |
| artemis | | 192.168.95.200 |
| apollo | | 192.168.95.201 |

SSL Certificates

| Cert | Issuer | Purchaser | Expiration Date |
|--------------------------------|------------|-----------|-----------------|
| aid.mlc-wels.edu | RapidSSL | Namecheap | Sep 2018 |
| *.mlc-wels.edu | PremiumSSL | Namecheap | May 2019 |

Orbeon Setup

Steps to Create an Orbeon App

CWDB

- Create needed schema and roles for new Orbeon app.

```
-- create user for Orbeon to use
CREATE ROLE orbeon_XXX LOGIN
    NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION;
-- create group for department users
CREATE ROLE XXX_forms
    NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION;
-- create the schema for forms to live in
CREATE SCHEMA orbeon_XXX AUTHORIZATION orbeon_XXX;
-- set the search path for the user Orbeon will be using
ALTER ROLE orbeon_XXX
    SET search_path = orbeon_XXX;
-- grant admin user for campus DB admin access to forms
GRANT USAGE ON SCHEMA orbeon_XXX TO admin_general;
-- grant department users access to forms
GRANT USAGE ON SCHEMA orbeon_XXX TO XXX_forms;
-- grant access to campus DB admin for any additional tables created by admin user
ALTER DEFAULT PRIVILEGES IN SCHEMA orbeon_XXX
    GRANT SELECT ON TABLES
    TO admin_general;
-- grant access to department users for any additional tables created by admin user
ALTER DEFAULT PRIVILEGES IN SCHEMA orbeon_XXX
    GRANT SELECT ON TABLES
    TO XXX_forms;
```

- Set password for `orbeon_XXX` user in PGAdmin.
- Login: `psql -U orbeon_XXX -h database.mlc-wels.edu cwdb`
- Check search path with: `show search_path;`
- Grant additional permissions by pasting in SQL statement below as `orbeon_XXX` user

```
-- grant access to campus DB admin for any additional tables created by orbeon_XXX user
ALTER DEFAULT PRIVILEGES IN SCHEMA orbeon_XXX
    GRANT SELECT ON TABLES
    TO admin_general;
-- grant access to department users for any additional tables created by orbeon_XXX user
```

```
ALTER DEFAULT PRIVILEGES IN SCHEMA orbeon_XXX
GRANT SELECT ON TABLES
TO XXX_forms;
```

- Paste edited schema definition from https://github.com/orbeon/orbeon-forms/blob/master/src/resources/apps/fr/persistence/relational/ddl/postgresql-4_8.sql (edited copy in `/root/orbeon/conf`)
- Add `, pk serial primary key` to each table def
- Add access rules to `pg_hba.conf` on CWDB and reload postgresql service configuration

OES

- Create group `OrbeonXXX.groups.ac.mlc` in iManager

Orbeon Server

- Alter Orbeon config files in `/root/orbeon/config`
- Create database resource in orbeon `context.xml`
- Add role assignment in Orbeon `form-builder-permissions.xml`
- Add orbeon persistence connection in `properties-local.xml`
- Add role to `oxf.fr.authentication.container.roles` in `properties-local.xml`
- Add role name to `auth-constraint` in `web.xml`
- Add role name to `security-role` in `web.xml`
- Check for active orbeon user sessions: <http://orbeon.mlc-wels.edu:8080/manager/>
- Re-deploy Orbeon

```
cd /root/orbeon
bin/deploy.sh war/current_link.war
service tomcat restart
```

Daily Ops Duties

This lists the daily tasks done by operations personnel on campus.

Backups

Internal Backups

Weekdays

- Verify that the prior backup was successful
- Swap the backup tape with the tape labeled for the **NEXT DAY**
- Log into `Portal` and `CWDB` and copy backups via SFTP to `ADMIN/Vol1/ServerBackups`

Weekends

- Label tape with date for the next Saturday
- Swap the backup tape with the tape you just labeled
- **ON SUNDAY**, swap the backup tape with the tape labeled for **MONDAY**

DMZ Backups

Weekdays

- Verify there are no errors from the prior backup
- Swap the backup tape with the tape labeled for the **NEXT DAY**

Weekends

- Use the `bctapelist` script to find which tape should be used next
- Swap the backup tape with the next tape from the `bctapelist` script

- Enjoy your weekend because you will not need to swap out a tape for this system until Monday

Support Tickets

1. Log into support.mlc-wels.edu
2. Look for new tickets that have not been assigned
3. Triage the tickets you can, assign tickets to those people who need them
 - **Password reset** requests are usually assigned to **Jill**
 - **Phone** issues and **signage** issues are assigned to **Jim**
 - **Database** issues start at **Laura**
 - **Portal** requests are assigned to **Aaron**
 - **Network, Server, and File Sharing** requests go to **Bob**
 - **Printer** issues start with **Ken**
 - **Notebook** and **desktop** issues start with **Ken**
 - **Paper** requests go to a **student worker**
 - **Website** issues start with **Bob**
 - **Website content** request go to **Sallie**
4. Just use your best judgement for others

XenServer Cluster Documentation

Internal Cluster

| Name | IP Address | Loc | OS | Ver |
|--------|--------------|-------------|-----------|-----|
| Zerah | 172.16.0.135 | Server Room | XenServer | 6.5 |
| Pharez | 172.16.0.134 | Chapel | XenServer | 6.5 |

General Network Info

- **Subnet:** 255.255.0.0
- **Gateway:** 172.16.1.2
- **DNS:** 192.168.95.100, 192.168.95.101
- **NTP:** oes.mlc-wels.edu, archive.mlc-wels.edu

External Cluster

| Name | IP Address | Loc | OS | Ver |
|---------|----------------|-------------|-----------|-----|
| Apollo | 192.168.95.201 | Chapel | XenServer | 6.5 |
| Artemis | 192.168.95.200 | Server Room | XenServer | 6.5 |

General Network Info

- **Subnet:** 255.255.255.0
- **Gateway:** 192.168.95.2
- **DNS:** 192.168.95.100, 192.168.95.101
- **NTP:** oes.mlc-wels.edu, archive.mlc-wels.edu

Storage Network

| Name | IP Address | Loc | Role |
|---------|---------------|-------------|---------|
| Jacob | 192.168.91.10 | Server Room | Storage |
| Esau | 192.168.91.14 | Chapel | Replica |
| Apollo | 192.168.91.30 | Chapel | Host |
| Artemis | 192.168.91.31 | Server Room | Host |
| Zerah | 192.168.91.21 | Server Room | Host |
| Pharez | 192.168.91.20 | Chapel | Host |

General Network Info

- **Subnet:** 255.255.255.0

XenServer Recovery and Other Things

Error: "VDI Not Available"

When a host box dies, often it will die without first notifying the rest of the hosts about the issue. In those cases VMs can get stuck and when you try and restart them you'll end up with the following error: `VDI Not Available`.

This sucks. Follow the steps on this page to correct it:

- <http://support.citrix.com/article/CTX138234>

Force VMs Down When Stuck

When a host box dies, often it will die without first notifying the rest of the hosts about the issue. In those cases, VMs can get stuck and are “missing” when viewed in XenCenter. You'll need to force them down so they show up again:

- <http://support.citrix.com/article/CTX126382>

Xen Appliance Conversion

From [Novell Cool Solutions](#).

1. Download the wanted Xen appliance from the Novell site. I chose iPrint 2 as my test appliance because I want to test iPrint.
2. Unarchive the download. You should have a folder with a raw disk image and a xenconfig file. My Filr disk image is 21+ GB in size once it is expanded. The xenconfig file is only 179 bytes.
3. Open your terminal application of choice and move into that newly created appliance folder.
4. Grab xva.py and drop it into the folder above the unarchived appliance folder. I used `curl` <http://www-archive.xenproject.org/files/xva/xva.py> but you better just [grab it from here](#).
5. Now is the fun part. Make sure you have enough free disk space to handle making a copy of the disk image. Also, make sure that xva.py is within that appliance folder. It will just make things easier.
6. Next I ran the following: `python xva.py iPrintAppliance-2.0.0.529/iPrintAppliance.x86_64-2.0.0.529.xenconfig -d iPrintAppliance-2.0.0.529/iPrintAppliance.x86_64-2.0.0.529.raw -f iPrintAppliance-2.0.0.529.xva` which will inspect the image and then output the whole thing as an XVA for import into XenServer. The xenconfig file contains the name of the disk image and other parameters needed, but there is the possibility you will need to include the disk anyway.

Troubleshooting

- You might need to use the `-d` flag to specify where to find the raw disk

CWDB Dev Server Refresh Scripts

The instructions below have been turned into two scripts. The refresh calls sync.

```
cwdb-sync.sh
cwdb-refresh.sh
```

CWDB Dev Server Refresh Instructions

```
# on the dev server
# ssh root@cwdb-dev

# sync
rsync -avz archive@cwdb-archive.mlc-wels.edu:cwdb/data `date +"%y-%m-%d"` /var/lib/pgsql/data_new
rsync -avz archive@cwdb-archive.mlc-wels.edu:cwdb/wal/ /var/lib/pgsql/archive

# refresh
rcpostgresql stop

rm -r /var/lib/pgsql/data/pg_xlog
rsync -av /var/lib/pgsql/data_new/ /var/lib/pgsql/data

mkdir -m 700 /var/lib/pgsql/data/pg_xlog
mv /var/lib/pgsql/data/postgresql.conf /var/lib/pgsql/data/postgresql.conf.prod
mv /var/lib/pgsql/data/postgresql.conf.dev /var/lib/pgsql/data/postgresql.conf
mv /var/lib/pgsql/data/recovery.conf.dev /var/lib/pgsql/data/recovery.conf

cp /var/lib/pgsql/data/SuSEfirewall2-custom /root/bin/SuSEfirewall2-custom
SuSEfirewall2

chown -R postgres:postgres /var/lib/pgsql/archive
chown -R postgres:postgres /var/lib/pgsql/data

rcpostgresql start
```

```
rm /var/lib/pgsql/data/recovery.done
```

Old Instructions

- install PostgreSQL server packages for your OS
 - `zypper in postgresql-server postgresql-contrib`
- start up PostgreSQL on OS (to create default directories)
 - `rcpostgresql start`
- you'll need to move the full data backup from `cwdb-archive` to `cwdb-dev` and replace all of the contents of the `/var/lib/pgsql/data` directory (we keep a number of days back)
- copy over wal directory from `cwdb-archive` to `cwdb-dev` and place it in the `/var/lib/pgsql/data` directory
- create `pg_xlog` directory
 - `mkdir /var/lib/pgsql/data/pg_xlog`
- make sure that everything in the data directory is owned by `postgres:postgres` with `700` permissions
 - `chown postgres:postgres`
- make certain to open the PostgreSQL Server ports in the firewall

FreePBX

SSH

- 172.16.0.148
- password safe

GUI

- <http://172.22.1.10>
- mlcasterisk:GdtbaKGdtbaK

E911

Any time an extension is *moved* to a different location, or if a new extension is *created*, the e911 information for that phone extension needs to be checked. **Background:** The campus has been divided into zones for the purpose of locating where a 911 call originated. Each zone is associated with an “Emergency Caller ID” that is assigned to each phone located in that zone. That Emergency CID needs to be entered into the configuration for each extension. The Emergency CID is a Direct Inward Dial (DID) of an assigned phone in that zone. Each room on campus is assigned a zone number in the public.rooms table of the Campuswide Database (CWDB). The public.valEmergencyZones table has the EmergencyZone_Name, EmergencyZone_Location, EmergencyZone_Comments, and the DirectDial_ID for each zone.

Comcast Documentation and Information

Here is information about current Comcast/XFINITY setup on campus related to connectivity.

Metro-E Service

- **Phone #:** (800) 741-4141
- **MLC Account #:** 930-000-194
- **MLC Phone #:** (507) 354-8221
- **MLC Address:** 1995 Luther Ct, New Ulm, MN 56073

XFINITY on Campus Circuit

- [Circuit Information](#)
- [Circuit Diagram](#)

Updating the Call List on Call Day

Update the *Calls & Assignments* page on the website:

1. Log into <https://mlc-wels.edu/login> with your MLC WordPress Account
2. Navigate to <https://mlc-wels.edu/assignments/> and click `Edit Page` in the top toolbar
3. Change the link for *May* under *2017* to <https://mlc-wels.edu/static/may-2017.pdf> (this link will not be live yet)
4. Click on *Update* to save the changes

Move Call Day List to Proper Location

1. Log into `mlc-wels.edu`
2. Copy PDF from `root` to `static` directory: `cp /root/may-2017.pdf /srv/www/htdocs/mlc-wels.edu/static/`

Moodle

- MyLab & Mastering Tools
- Automatic, based on tool URL
- <https://tpi.bb.pearsoncmg.com/highlander/api/o/lti/tools>
- martinluther.moodlelti.com
- KsHKyCKe
- <https://moodle.mlc-wels.edu/moodle/blocks/mylabmastering/pix/icon.jpg>

Student Worker Admin Accounts

| Account | Student | Assigned |
|-----------|-------------------|----------|
| bilbo | | |
| camellia | Eric Bartsch | 20200929 |
| samwise | Benjamin Haferman | 20220518 |
| gaban | Caleb Carlovsky | 20210818 |
| galadriel | Alison Foxen | 20220518 |

Network Services Admin Accounts

| Account | Person | Assigned |
|----------|----------------|----------|
| arwen | Laura Stelljes | |
| eowyn | Jill Roux | |
| gaban | AVAILABLE | |
| galadrie | AVAILABLE | |
| gandalf | AVAILABLE | |
| laker | James Rathje | |
| legolas | Bob Martens | |
| merlin | AVAILABLE | |
| modred | Ken Jones | |
| sauron | Aaron Spike | |

Trane Cloud VPN

Branch Office Gateway

- **Local Network:** 10.11.150.0/24
- **Local Gateway:** 10.11.150.2
- **Remote IP:** 52.43.55.153
- **Remote ID:** 10.242.202.66
- **Pre-Shared Key:** SEE PASSWORD SAFE
- **Version:** IKEv1
- **Phase 1 Transform:** SHA1-AES (256-bit)
- **Phase 1 Key Group:** DH Group2

Branch Office Tunnel

- **Tunnel Local Addresses:** See Local Network
- **Tunnel Remote Address:** 10.242.202.101/32
- **Phase 2 PFS:** DH Group2
- **Phase 2 IPSec Proposal:** ESP-AES256-SHA256

More Information

Use the wizard to setup the default BOVPN rules (using an All set) and then modify them for only the Trane VLAN and turn on logging for all rules. You may need to re-key the VPN if you make any changes.

Goats

Stolen from

https://www.reddit.com/r/sysadmin/comments/4l7kjd/found_a_text_file_at_work_titled_why_should_i/.

- Found a text file at work titled “Why should I quit my job and become a goat farmer? (written during my “on-call” week)”
- You don't have to monitor the utilization on a goat.
- Milk a goat and the goat stays milked for a while.
- There are no 32-bit goats.
- You don't have to do a demo on a goat. And if you ever do, the goat will do what it's supposed to do and there's not a lot that can keep it from doing it.
- When a goat goes “down”, you just bury it and buy a new goat.
- Left alone, Billy goats and Nanny goats do what they're supposed to do. You don't need to format them, monitor them, be on-call for them, step, trace or inspect registers.
- Nobody cares if you're not a Certified Goat Engineer yet.
- Kill a goat to make a goat steak, and the goat stays dead.
- Most people will take advice from a goat farmer on how to paint a fence, cook a steak, fix a tractor, etc. but most people somehow just don't want to hear it from a computer weenie.
- Nobody can lie in a job interview about their goat experience.
- Goats don't page you.
- When it comes to “software” (food), EVERYTHING is compatible with a goat.
- You don't need to buy a “goat 98” to fix all the bugs in your goat 95
- You can tell whether a goat has been “debugged” by looking at it.
- Goats don't become obsolete. If they do, as long as you didn't neuter them, they make the necessary upgrades themselves.
- No commute.
- Goats are kind of cute. Computers aren't cute unless they're Macintoshes, and those are just plain annoying.
- No dress code. Of any kind. EVER.
- You always have the right “file permissions” to milk a goat.
- If a goat gives too many timeout errors, or does not avail you resources for your session, or if performance is generally slow for your applications on your goat, it just means you're having goat steak for dinner.
- You don't need to visit “shareware dot com” to get some tools to milk a goat. You either have your bucket or you don't.
- The bucket leaks, or it doesn't. You do not need to ask a network if you're still the owner of the bucket. You do not need to run a bucket compare against a copy you made of the bucket previously You couldn't care less about the checksum of the bucket.
- You don't need to “free up some megs” before you milk a goat.

- You get callouses on your hands - the way God intended!
- You don't need to call a staff meeting to make sure everyone's milking goats the same way.
- Nanny goats, with no TCP/IP stack loaded, and no DLC, still give milk.
- Just about any barnyard animal is fault tolerant (except some cows).
- You don't need to sign in with the front desk if you need to milk a goat on a weekend. You don't need to use a badge to open a front gate. If you find an empty coffee pot burning on the machine on a Saturday, you just yell at your wife.
- You don't need to worry if you've been spending a lot of time milking what you will later find out to have been an improperly labelled "development goat".
- There is no such thing as a "preferred goat," and your "goat context" is always correct. Passwords do not exist and your milking/slaughtering account will never be disabled because of intruder detection.
- Carpal tunnel is guaranteed. Don't worry about it.
- A goat has all the "patches" it will ever need. If it doesn't it just means you're having goat steak for dinner.
- Goats that become full do an automatic "core dump" but they take care of getting themselves reset and on-line. You just have to clean up. You do not need to worry about defragmenting or compressing the goat. The goat does not have to be zipped, archived or converted to Goat-32.
- As long as the stable hasn't caught fire, a goat couldn't care less about a power surge.
- Goats don't have to be backed up at night.
- Each and every one of the parts of a goat use the same interrupt, and the goat works just fine anyway.
- A goat is a goat is a goat.
- You don't EVER restart a goat. You do shut them down sometimes and it's the first step in many of your recipes.
- Nobody ever needed to draft up a goat-milking requirements document.
- You deliver applications to goats. Goats do not deliver applications to you.
- A goat will do practically anything to get more comfortable. Computers have been known to display the same error message over and over again, all day, without regard to how frequently or how hard the monitor has been hit, slapped, punched or kicked.
- You don't have to log off of a goat and listen to some silly "Exit Goat" sound effect for the next several minutes.
- You won't find out from your next phone bill that you milked your goat too much for your budget.
- On a goat, the SYS\$ERR.LOG file is ALWAYS EMPTY.
- Operating systems come & go, but goats will probably never be "orphaned" as they are expected to be produced by their manufacturer for quite some time to come.
- There are no workstation licensing issues with goats.
- You don't get in trouble for milking a goat during business hours, and nobody cares if you reformat it.
- If it's late and you have a lot of goat-milking to do, at least you can see your kids before they have to go to bed. You can probably even make them help you milk your goats.
- You don't need 32 megs of RAM to get started milking your goat.
- Goat security is applied completely, thoroughly, and with all the features you'll ever need, using a stake and a rope.

- Nobody ever got a general protection fault milking a goat.
- You don't need to worry about your whole goat herd locking up if you put an ethernet goat and a token-ring goat together in the same stable.
- You don't name goats. If you do name goats, you can give two or more goats the same name and this will not interfere with your ability to access any of the goats.
- Your kids will not meet some pervert who wants to buy them a bus ticket when they play with a goat.
- There is no closely-watched dispute between Microsoft and any competitor, over who will dominate the goat-milking product industry. You will probably never be asked to check-mark a box that says, Make this my default goat-milking bucket.
- You do not want, need, or desire in any way for goats to run at a higher clock speed. And they don't.
- You do not need to use a wrist strap to ground yourself before milking, and there's never a need to put your goat in a little plastic baggie. Unless making goat steak
- There really aren't too many ways to improperly shut down a goat.
- Surrounded by a room full of younger goat farmers, you don't need to worry about dating yourself talking about 300-baud or 4.7-Mhz goats.
- y2k.
- You do not need to buy anything to "uninstall" a goat. Maybe a gun or a knife.
- Once you've filled a bucket with goat milk, the goat can crash and it doesn't matter whether you've "saved" or not. Just don't spill.
- When you buy a new goat, the goat does not need to re-write registry keys on the farm that could have unforeseen effects on the other animals already residing there.
- There are no easter eggs in a goat.
- Your wife will never yell at you for removing all of the RAM from her goat.
- You never need to learn Goat 2000, Goat Perfect 8, or Goat 123
- You don't need an Internal IPX Address to boot a Goat.
- Goats don't need a per-bucket license.
- You will never spend 4 hours upgrading a goat over the wire.
- There is no Goat Ops.
- Goats follow upgrade procedures.
- Goats eat org charts.
- If a goat gets an uncleanable virus, you shoot it.
- If a goat has a non-terminal virus it just does the poo-poo.
- Goats don't need pagers and never get a 'please advise'.
- Goats don't have to worry about whether or not it's Calcomp.
- A goat farmer doesn't care if people can't remotely access his herd.
- No MHN Goat herd.
- No one gives a rat's ass if the goats aren't talking to each other.
- Ever heard of a proprietary goat?
- No goat analysis meetings.
- No goat control meetings.
- No meetings.
- Goats will never need service pack 4.
- No DS problems at GOATADRIVE.
- You fuck the goat, he doesn't fuck you and the whole department.
- A goat might bite you in the ass, but he won't fuck you.

- Fuck Y2K.
- Goats don't ever ask stupid questions.
- Goats don't drive technology dollars away from your automobile lusts.
- If a goat takes a "dump" in the middle of the night, you take care of it when you damn well feel like it.
- Nobody will fire you for connecting "diskless goats" into a "goat server" when they think you should have purchased a massive mainframe goat to connect to a multitude of inexpensive "dumb goats".
- ISO is not publishing any standards about how you should be farming your goats.
- Counting from zero instead of one, doesn't apply to anything goat farmers do and looks stupid. Hexadecimal is unheard of.
- When you sell a goat, you don't need to export it to a format that will be understood by the buyer's ancient goat-reading software.
- All your stuff will still work when you buy your 100th goat, and your 256th goat, and your 65,536th goat...
- People don't walk up to goat farmers at parties and whine about how they just got a French Alpine and don't know how to milk it.
- Nobody can go through your goat and get you in trouble for what they find in there.
- You don't have to administer a "user acceptance test" when you deliver goat cheese.
- You don't need any special utilities to delete a goat that is not empty.
- You don't need or want goats on your desktop, or shortcuts to goats on your desktop. Most goat farmers don't have desktops.
- Nothing a goat farmer does requires a mouse. If you have mice you get a cat.
- Goat farmer error messages: Goat not found; Goat dead; Goat not awake; Too soon after last milking; Billy goat detected. That's about all. You don't need silly numbers for these, and you don't need to look them up anywhere or check them out at goat.com.
- There are no read-only oats. There are no hidden or system goats.
- You don't need to mail anyone a core dump from a goat to fix a problem. The only time you would do this is to CAUSE a problem.
- A goat that doesn't know what time it is will work just fine.
- A goat that is not Y2K compliant will simply think it's not Y2K. This is doesn't even require documentation.
- If your spouse doesn't authorize the purchase of a new goat, you simply encourage your goats to make one from existing parts.
- A goat doesn't have enough fingers to press <shift><Shift><Ctrl><Alt><Esc>
- Goats don't argue about it being another goats problem. They just kick each others ass.
- If a goat had to document every time it took a shit, we would be out of forests.
- Goats don't give a shit about email.
- The only way a goat can deliver an 'application' is through it's ass.
- Goats can't get there benefits revoked they are just made into goat steaks for dinner.
- A goat farmer doesn't have to provide documentation on his goat's ability to produce milk after the year 2000.
- GoatEng.
- Macintosh goat users will not make fun of you because your goat is more problematic & complicated than the goat they just bought.
- Goat farmers who voted for Perot have pretty much the same type of goat as everyone else, so they can go back to arguing about politics like they were doing before 1984.