

EquipmentBarn.com Procedures Document

This document will describe the steps necessary to keep EquipmentBarn running smoothly and what to do when something doesn't go smoothly. This is necessary because I don't have great long-term memory ☺

The 1st section includes the weekly steps to do things like backups, log and cron job monitoring, etc. The second section includes the more serious things like how to failover and recover from an outage, copy a database between 2 PC's.. etc.

Contents:

Ongoing Operations

- Backups

- Log Monitoring

- Cron job monitoring

Specialty Procedures

- Taking A Short Outage

- Production Failover/Failback (for longer term outages)

- Copying Databases between PCs

- Deploying Code

- Building/Rebuilding a server

- Locking the Server Down

- Configuring Terminal Server

Ongoing Operations

Daily Monitoring

Daily Backup/Validation-Cron this somehow? Send test logs to prod & prod to test?
Look for anything other than port 80 in the web logs

Weekly Tasks

Look for repeated logins in web logs and security logs

Monthly Tasks

Backup System Data-Test to prod & prod to test (P.183 in IIS Security Book)
Full Database Backup-Burn a copy for offsite
Archive & Reset the security logs

1) Database Monitoring (every couple days)

Validate that email message are changing to “sent”, look in the outbox of the Qmail users to validate
Validate new records in the eb_usage table
Look at the eb_joblist table to make sure stuff is accumulating there
Look at the eb_statistics to validate that info is accumulating there

2) Backups (frequency & approach TBD)

Backup the database
Backup the /EB/EBFilesystem/EBSiteSessions.txt file
Backup any necessary log files

3) System/Log Monitoring (every couple days)

Look for any suspicious hacking- web server logs, security logs (i.e. repeated logins)
Look for large variances in size- web server logs
Look for errors in application logs
Check disk space
Look for Google and Yahoo bots

4) Cron Job Monitoring (at least once a week)

Look at Cron.log file in the logs folder
Look for general errors and to make sure the jobs have been running
Look in the scheduler for error on last run?

5) Data Cleaning (yearly? As needed-maybe more often on weblogs)

Archive off web logs
Archive eb_email table
Archive EBCron.log
Archive eb_joblist table?
Clean sent items from Linux box?

Specialty Procedures

How to take an outage

- 0) Check for connected users? Wait depending upon reasons.
- 1) Temporarily redirect both port 80 or 81 (or both if necessary) to the Linux box (or backup box)
- 2) Pause any cron jobs scheduled to run during outage
- 3) Stop any Web services applications
- 4) Stop EB application
- 5) Stop database if necessary
- 6) Do required maintenance
- 7) Restart DB
- 8) Restart Web services
- 9) Restart EB Application
- 10) Manually run any cron jobs that needed to be run during outage timeframe
- 11) Redirect both ports 80 or 81 (or both if necessary) back from backup box
- 12) Run RefreshAsp.pl to pre-compile pages

How to do prod failover to test (for extended outages)

- 1) Check for connected users? Wait depending upon reasons.
- 2) Temporarily redirect both port 80 or 81 (or both if necessary) to the Linux box (or backup box)
- 3) Pause any cron jobs scheduled to run during outage
- 4) Stop any Web services applications
- 5) Stop EB application
- 6) Stop both SQL Server Instances
- 7) Copy the database files/data to test as necessary (see process below for copying a database)
- 8) Remove the EBUser from the EB database (but not the instance)
- 9) Re-Add the EB User to the EB database
- 10) Copy the EB/Filesystem directory and possibly logs? Dir to new machine
- 11) Update any EB_ environment variables (for test/dev environments, etc)
- 12) Remove the -T test flag on the eb_email.pl cron job
- 13) Save the current web.config test file
- 14) Update the web.config file to match new machine settings
- 15) Restart DB
- 16) Restart Web services
- 17) Restart EB Application
- 18) Manually run any cron jobs that needed to be run during outage timeframe
- 19) Redirect both ports 80 or 81 (or both if necessary) back from backup box to the new box
- 20) Run RefreshAsp.pl to pre-compile pages

How to do prod fallback from test (recover from extended outages)

Run the steps just as above but move from DEV to prod, should not need to update env var's back on prod box

Reset the env vars and web.config (copy) back to the original values on the test box (including the -T flag on eb_sendmail)

*Note that it should also be possible to only take a database only outage by changing the database environment variables (documented above) and restarting the application(s)...or a web server only outage by redirecting the port and changing the EB_DATABASE environment variable and restarting the application on the other server.

How to copy a database between PCs'

- 1) Shut both down
- 2) Copy the data files over
- 3) Remove the EBUser from the EB database (but not the instance)
- 4) Re-Add the EB User to the EB database
- 5) Restart Both Databases

Moving Code Between Environments/Deploying Code

- 1) If this is a new release create a checkpoint in source safe
- 2) Stop the web server
- 3) Copy the page files
- 4) Copy the cron job perls
- 5) Copy any necessary/changes Graphics/Include files, etc.
- 6) If copied Web.config then don't forget to uncomment the correct set of vars for the environment
- 7) If copied the /Filesystem directory be sure and reset or update any session counter file(s)
- 8) Run RefreshAsp.pl to pre-compile pages

Steps for building/(rebuilding) a server (assuming not just restoring a ghosted image):

- 1) Backup IIS configuration, Backup scheduled tasks
- 2) Disconnect IIS from web (I.E. make sure ports are mapped to another box and no redirections running)
- 3) Install Win2000 Server (select to install IIS)
- 4) Apply all service packs and windows updates
- 5) Install the .Net framework
- 6) Install SQL Server
- 7) Install SQL Server Service Packs and Windows Update again
- 8) Run NTFckUp thingy to make sure things are up to date
- 9) Restore IIS configuration-or create apps again. (See Steps Below)
- 10) Restore cron jobs
- 11) Run the IIS lockdown tool?
- 12) Restore the Application Code and Necessary Files
- 13) Start and test the application(s)-See test document-including WebServices stuff
- 14) Run RefreshAsp.pl to pre-compile pages
- 15) Depending on machine install and configure Terminal Server client and/or Server

Locking Down a Windows Server & IIS. (references are pages in ISS Security Book)

- 1) Run IIS Lockdown Tool
- 2) Run Microsoft Security Baseline Analyzer
- 3) Stop any unnecessary services-P.72 for a list of minimum required
- 4) Disable Parent Paths-P.77
- 5) Remove Mapping-P.79,82 (header)-Checklist on P.91
- 6) Remove Everyone privilege to control drives (remove all from root and add back for each user)
- 7) Rename Administrator account
- 8) Remove guest account from guest group (P.121)
- 9) Rename IUSR_* account-remove ALL permissions except what required on a couple directories
- 10) Create new group siteguests-create new guest account(P.123)-Explicitly deny all & then add back
- 11) Remove guest account from Local Security Policy-P.126
- 12) Run scan/hack utilities on P.209-verify logs catch the entries
- 13) Add evens on P.210 to monitor procedures
- 14) Set security log file size (& location?)-P.145
- 15) Read through local & account options in security settings in MMC
- 16) Change all log file permissions P.152-155
- 17) Rename or remove & backup extra SAM file on \Restore Directory
- 18) Make registry backup
- 19-24) Private

Periodically:

Watch www.sans.org/top20.htm

Run Microsoft Security Baseline Analyzer (MSBA)

Run HFNetCheck (Subset of MSBA?)

Test Box Only

Disable IUSR_* account and add a tester account w/UserId & Password-Lock the test account down well!

Remove guest account entirely

Notes:

NEVER assign write and execute permissions on the same directory

In event of an attack:

- 1) Disconnect from Internet & rest of network
- 2) Analyze-look to see if other machines compromised
Step back through logs from where first noticed back to login to determine hack point
- 3) Reinstall-change all passwords on all machines-even those not hacked
- 4) Patch hole that was compromised

Steps for configuring IIS:

- 1) Add a mapping in for .shtml files (if used on the site) to ssinc.dll (documents->configuration to get to mapping)
- 2) Create forwarding sites & forward proxies (test->prod and prod->test)

Steps for installing and configuring Terminal Server:

- 1) Install the Terminal Server software and change the port to be the appropriate one for machine
HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
3373 for Prod (10.0.0.3 machine) & 3374 for Test (10.0.0.4 machine)
Reboot
- 2) Install the Terminal Server client from the floppy (Windows 2000 only-XP has built in and allow port after name)
- 3) Create a new connection in the client connection manager and go to File and export the connection
- 4) Open the text file created by the export and update the Port #
- 5) Import the connection over the other one