JBoss Certified Technology Partner

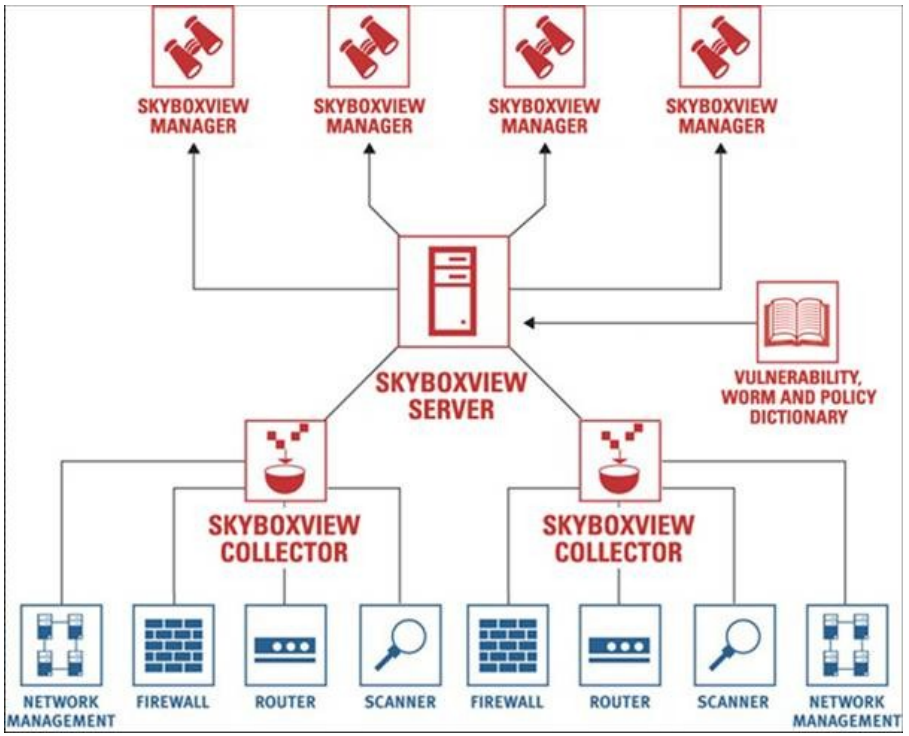
Israel JBoss User Group

Session 03 / 14.8.2006

JBoss Usage in Skybox

By : Yair Shmueli Skybox Security

Component Architecture



Model Management

Skybox View - Live Model

File Edit View Insert Tasks Access Tools Host Help

New | Network Map | Access Analyzer | Attack Explorer | Live | skybox security

Skybox View

Security Analyses
Access Policy
Organization
Tickets
Reports

Organization
- Business Units & Assets
  - Asia-Pac Operations
    - Regional gateway
    - Regional servers
  - Europe Operations
  - US Headquarters
    - Corporate Service
      - Production DB
      - Production We
    - IT
    - Los Angeles
    - New York
- Locations & Networks
  - Europe
    - London
      - gatewaysNort
      - gatewaysNort
      - financeWindo
      - financeUnixW
      - financeServer
    - Paris
      - gatewaySouth
      - gatewaySouth
      - developmentV
      - developmentL
      - developmentS
  - Resellers
  - US
  - 16.0.0.0 / 8
  - Backbone[192.170.8.(
  - 200.160.2.0 / 24
  - Internet[cloud]
  - Unassigned Hosts
- Zones

financeServers[192.170.27.0 / 24] Hosts

Hosts | Network Map

Name	IP Address	OS	OS Version	S...	Creation Time	Modificatio...
Finance Router	192.170.27.1	IOS		Up	9/17/03 4:2...	6/25/06 11...
finance_server_0	192.170.27.2	AIX	3.2	Up	9/17/03 4:2...	6/25/06 11...
finance_server_1	192.170.27.3	AIX	3.2	Up	9/17/03 4:2...	6/25/06 11...
finance_server_2	192.170.27.4	AIX	3.2	Up	9/17/03 4:2...	6/25/06 11...
finance_server_3	192.170.27.5	AIX	3.2	Up	9/17/03 4:2...	6/25/06 11...
finance_server_4	192.170.27.6	AIX	3.2	Up	9/17/03 4:2...	6/25/06 11...
finance_server_5	192.170.27.7	AIX	3.2	Up	9/17/03 4:2...	6/25/06 11...
finance_server_6	192.170.27.8	AIX	3.2	Up	9/17/03 4:2...	6/25/06 11...
finance_server_7	192.170.27.9	AIX	3.2	Up	9/17/03 4:2...	6/25/06 11...
finance_server_8	192.170.27.10	AIX	3.2	Up	9/17/03 4:2...	6/25/06 11...
finance_server_9	192.170.27.11	AIX	3.2	Up	9/17/03 4:2...	6/25/06 11...
finance_web_0	192.170.27.12	Windows...	Server SP 4	Up	9/17/03 4:2...	6/25/06 11...
finance_web_1	192.170.27.13	Windows...	Server SP 4	Up	9/17/03 4:2...	6/25/06 11...
finance_web_2	192.170.27.14	Windows...	Server SP 4	Up	9/17/03 4:2...	6/25/06 11...
finance_web_3	192.170.27.15	Windows...	Server SP 4	Up	9/17/03 4:2...	6/25/06 11...
finance_web_4	192.170.27.16	Windows...	Server SP 4	Up	9/17/03 4:2...	6/25/06 11...
finance_web_5	192.170.27.17	Windows...	Server SP 4	Up	9/17/03 4:2...	6/25/06 11...

31 Hosts

Host: finance_server_0 [192.170.27.2]

IPS Rule Groups | Routing Rules | Vulnerabilities | Attacks | Tickets

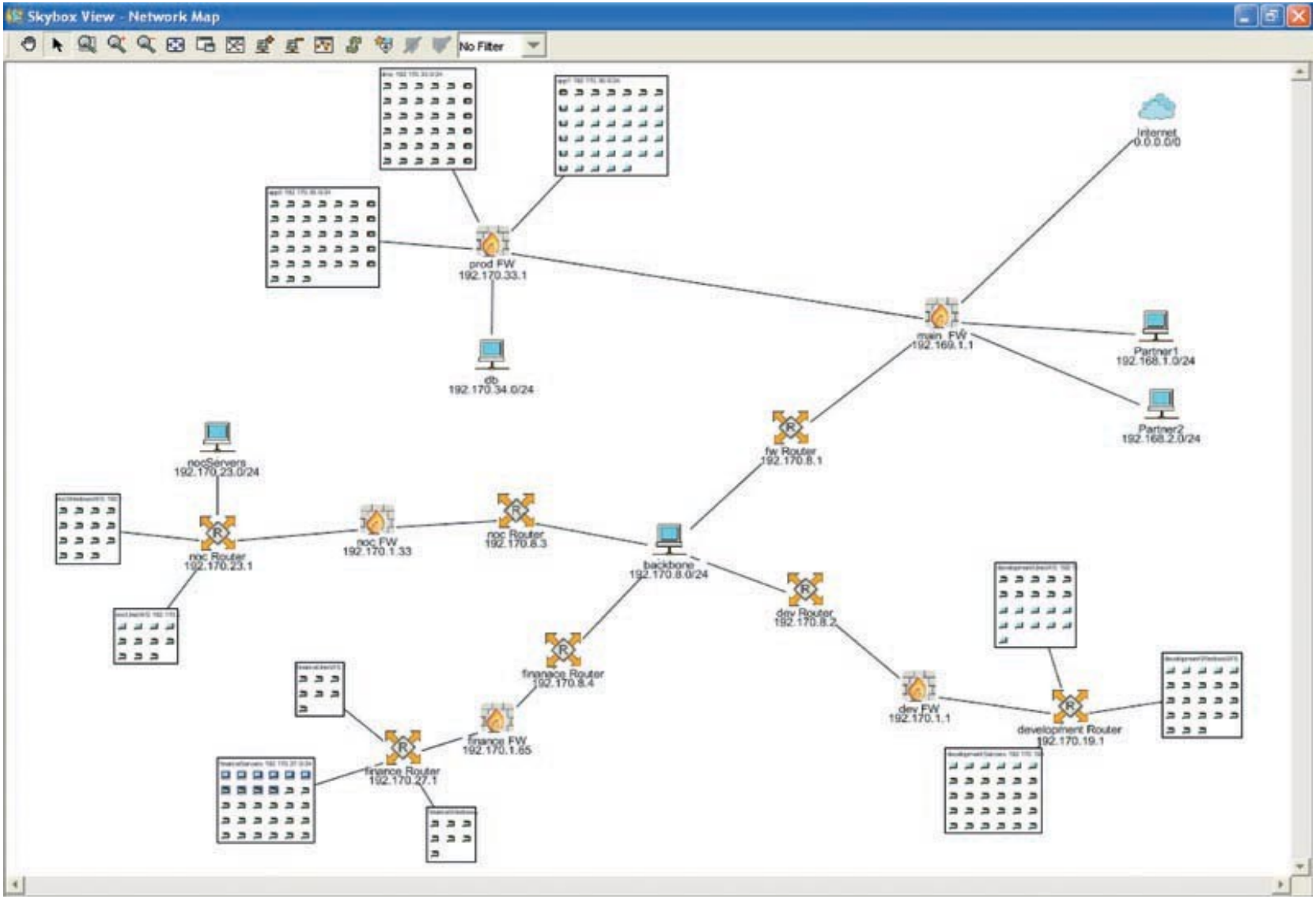
General | Services | ACL Rules

Name	Type	Vendor	Ports	Version	Status
AIX (Unix OS)	OS	IBM		3.2	Up
ColdFusion Server (col...	Remote	Allaire	8500/TCP		Up
AIX (ftp)	Remote	IBM	21/TCP	3.2	Up
ssh (ssh)	Remote	Generic	22/TCP		Up

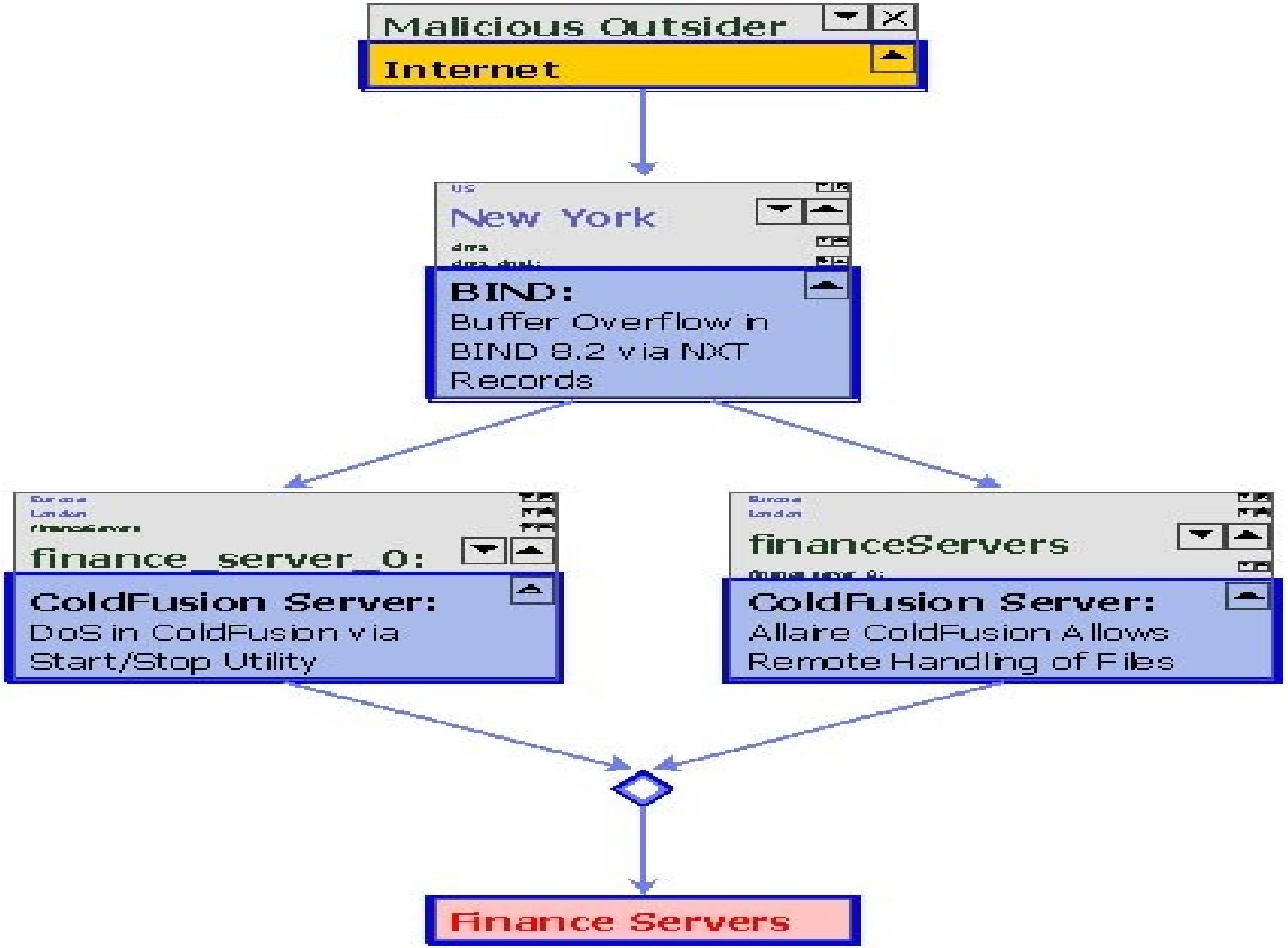
4 Services

No running tasks | User: skyboxview | Server: localhost:8443

Normalized Network Model



Attack Simulation



FW Configuration Change Assurance

ACL Rule Differences

main FW [192.169.1.1]

Access | NAT

Live

#	Source	Target	Services	Action
1	Any	Network dmz	Any	✓
2	Network deve...	Any	Any	✓
3	200.160.1.0-2...	192.170.30.0-...	135/TCP	✓
4	Network Inter...	Network deve...	FTP, telnet	✓
5	Network finan...	Network Inter...	Any	✓
6	Network Part...	Host group Pr...	DB	✓
7	Network Part...	Host group Pr...	Any	✓
8	192.168.1.0-1...	192.170.36.0-...	135/TCP	✓
9	192.170.36.0-...	192.170.21.0-...	80/TCP, 135/T...	✓
10	Network deve...	Host group All...	FTP	✓
11	192.170.25.0-...	192.170.34.0-...	135/TCP	✓
12	192.170.33.0-...	192.170.27.0-...	8500/TCP	✓
13	Any	Any	Any	✗

What If

#	Source	Target	Services	Action
1	Any	Network dmz	80/TCP, 21/TC...	✓
2	Network deve...	Any	Any	✓
3	200.160.1.0-2...	192.170.30.0-...	135/TCP	✓
4	Network Inter...	Network deve...	FTP, telnet	✓
5	Network finan...	Network Inter...	Any	✓
6	Network Part...	Host group Pr...	DB	✓
7	192.168.1.0-1...	192.170.36.0-...	135/TCP	✓
8	192.170.36.0-...	192.170.21.0-...	80/TCP, 135/T...	✓
9	Network deve...	Host group All...	FTP	✓
10	192.170.25.0-...	192.170.34.0-...	135/TCP	✓
11	192.170.33.0-...	192.170.27.0-...	8500/TCP	✓
12	Any	192.170.34.35	1433/TCP	✓
13	Any	Any	Any	✗

Close | Next Change | Previous Change | Show | Original ACL Text | Changed

Technology Overview

- JDK 1.2 -> 1.3 -> 1.4 -> 1.5
- JBoss 3.0.3 -> 3.2.1 -> 4.0.3SP1
  - Tomcat
  - JMS
  - JTA
  - Connection Pool
  - JNDI
  - JAAS
  - Axis
  - Log4j
  - RMI for shutdown
  - EJB 2.1 CMP entity beans
  - EJB 2.1 Stateless session beans
- Server & collector both use JBoss but configured differently

MySQL

- MySQL 3.23 -> 4.0 -> 4.1 -> 5.0
- 100 model tables x 3 workspaces + 30 core tables
- Some tables can reach 1M records
- Using Innodb engine
- Transparent JBoss-MySQL integration
  - Shared installation
  - Shared lifecycle: startup/shutdown
  - Schema creation on JBoss startup (and upgrade)
  - Initial data creation on JBoss startup (and update)
- New in MySQL 5.0 - Connector/MXJ MBean
- No stored procedures & triggers prior to 5.0
- No sub-selects prior to 4.1
- Backup & restore
  - mysqldump – assumes unchanged schema on restore
  - Zipped encrypted XML
    - Bouncy Castle JCE provider for PBE AES
    - Backward compatibility supports restore even when schema has changed
- UTF8
  - I18N, Japanese

Swing & Web client facade

- Business service Facade used by Swing client and Web client
- Similar infrastructure provides server -> collector invocation
  - Typically asynchronous activity
  - Management & monitoring API
- Implemented with EJB 2.1 stateless session beans
  - Transaction declarations - CMT
  - Role-based security declarations
  - Security proxies
  - Problem: descriptors get out-of-sync (Spring also problematic...)
- Our own remote method invocation
  - Java serialization over HTTPS
  - Simple, transparent, effective, firewall friendly
  - Serialization errors if server & swing client out-of-sync, requires automated software update
  - Client-side uses Proxy and Jakarta HttpClient
  - Server-side uses Servlets
  - Client-side and server-side SSL certificates
  - Local invocation
  - Web client calls facade from Struts controllers

Swing & Web client facade - cont

- DTO
  - Serializing DTO or DTO mini-graphs (View objects)
  - DTO responsible for loading itself from ResultSet
    - Supports joined results with table aliases
    - Column access utilizes cached indexes
  - DTO responsible for writing itself to CSV for MySQL load
  - DTO responsible for XML load & XML save
  - CMP entity bean utilizes DTO
  - Model graph utilizes DTO
- CMP
  - CMP entity beans < 5 entities, gave up on CMR strategies
  - JDBC > 5 entities
  - Create typically in CMP
  - Commit option B
  - JDBC modifications trigger flushing of JBoss cache
  - Descriptor mess (welcome JDK 1.5 annotations)
- Queries
  - EJB-QL for few legacy queries, JDBC for most queries
  - Complex queries with user-defined filters & sort criteria
  - Chunk-based retrieval using LIMIT
  - Runtime MySQL EXPLAIN to force index strategy
  - SELECT * can be slow, often selecting specific fields as needed
  - MySQL query cache – useServerPrepStmts=false in driver

Model Graph

- POJO model graph
- Utilizing same DTO used in facade
- Adds object relationships, analogous to CMRs
- Used for
  - Heavy-duty algorithms running as batch tasks in background
  - Server-side complex traversal algorithms for GUI components
  - Alternative: Facade, Stored procedures
- Optimized to hold full model in memory
- Generic load filters – by table, by field
- No lazy load
- Mass load via full table SELECTs
- Transparent persistence
  - Automated dirty checks on entities and relationships
  - Heuristics determines CRUD or total replacement
  - Creates & updates via LOAD DATA INFILE
  - Deletions via cascade deletes
  - Full table deletions with TRUNCATE are slow -> DROP TABLE
  - Null id marks new entities (similar to Hibernate)
  - id assignment relies on MySQL auto increment

Model Graph Cache

- POJO models cached per workspace
- Master model handoff on task sequences
- Cache totally invalidated on relevant Facade writes
- Application locks
  - » Protect DB resource on batch operations
  - » Allow concurrency of batch operations where possible
  - » 3 lock levels
    - multiple read locks
    - single update lock that allows read, can be upgraded to write
    - mutually exclusive write lock
- Facade mutators throw error when update/write lock is taken
- Facade accessors ignore these locks – might be problematic in rare cases

Memory Issues

- 2GB RAM windows –Xmx 1300M
- 4GB Linux Hugemem kernel –Xmx2600M
- 64 bit with JDK 1.5 on amd64, em64t
- Xmx setting should consider other processes on same machine
- MySQL takes less than 200M virtual memory (100+ connections)
- Permanent generation size 100M
  - Beware of String.intern()
  - Beware of misleading JDK 1.4 OOM errors
  - Swing GUI utilizes Low Pause GC
    - -XX:+UseConcMarkSweepGC
    - -XX:+CMSClassUnloadingEnabled
    - -XX:+CMSPermGenSweepingEnabled
- Beware of RMI full GC every minute in JBoss
  - -Dsun.rmi.dgc.server.gcInterval=0x7FFFFFFFFFFFFFE
  - -Dsun.rmi.dgc.client.gcInterval=0x7FFFFFFFFFFFFFE
- Observed long GC times in server
  - affected JDBC connections & GUI experience, OOM
- No beef with Sun's alternative GC algorithms and/or numerous options
- Eventually solved by explicit GC contrary to Sun guidelines
  - periodic (every 30 minutes)
  - pre/post certain memory intensive tasks
- GC and heap usage monitored in logs

Testing

- JUnit
- EJB 2.1 makes testing difficult – requires container
- Our server takes approx few minutes to start
- Hot deploy sometimes unpredictable
  - Beware of daemons
- Partial solution to EJB 2.1 testing
  - Stateless session beans are wrappers over POJO singletons
  - Junits configured to run with/without container
  - OK for JDBC but no solution for entity beans
- Server crashes
  - Be sure to track JDK update releases
  - Be sure to track Linux kernel bug fixes
  - Beware of JNI and 3rd party dynamic libraries
  - Never tracked a crash to JBoss itself