

Clinical Information Support System
Occupational Health Record-Keeping System

Production Operations Manual



September, 2011

Release 1.4

**Department of Veterans Affairs
Office of Information & Technology
Product Development**

Revision History

[illegible]

Table of Contents

1.	Introduction	1
1.1	Summary	1
1.2	Purpose	1
1.3	Scope	1
1.4	Related Documents and Agreements.....	1
1.4.1	Memorandum of Understanding (MOU)	1
1.4.2	Service Level Agreement (SLA).....	2
1.4.3	Service Level Requirements (SLR)	2
1.4.4	Operational Level Agreement (OLA)	2
1.4.5	Operations and Maintenance Plan (O&M)	2
1.4.6	Underpinning Contract.....	2
1.5	Section Summary	3
2.	System Business and Operational Description.....	3
2.1	Operational Priority and Service Level	4
2.2	Logical System Description	4
2.3	Physical System Description	4
2.4	Software Description.....	6
2.4.1	Background Processes.....	7
2.4.2	Job Schedules – (Reference Background Processes)	8
2.5	Dependent Systems	9
3.	Routine Operations	9
3.1	Administrative Procedures	10
3.1.1	System Start-up	10
3.1.1.1	Windows Database Server	10
3.1.1.2	Linux Web server:.....	10
3.1.1.3	Linux Application server:	11
3.1.2	System Shut-down	12
3.1.3	Back-up and Restore	15
3.1.3.1	Back-up Procedures	15
3.1.3.2	Restore Procedures.....	16
3.1.3.3	Back-up Testing	16
3.1.3.4	Storage and Rotation.....	16
3.2	Security / Identity Management	17
3.2.1	Identity Management	17
3.2.2	Access control	17

3.3	User Notifications.....	18
3.4	System Monitoring, Reporting & Tools.....	18
3.4.1	Availability Monitoring	19
3.4.2	Performance/Capacity Monitoring.....	20
3.4.3	Critical Metrics	21
3.5	Routine Updates, Extracts and Purges.....	21
3.6	Scheduled Maintenance.....	22
3.7	Capacity Planning.....	22
4.	Exception Handling	22
4.1	Routine Errors	22
4.1.1	Security	22
4.1.2	Time-outs	22
4.1.3	Concurrency	23
4.2	Significant Errors	23
4.2.1	Application Error Logs	23
4.2.2	Application Error Codes and Descriptions	23
4.2.3	Infrastructure Errors	23
4.2.3.1	Database	23
4.2.3.2	Web Server.....	24
4.2.3.3	Application Server	24
4.2.3.4	Network.....	24
4.2.3.5	Authentication & Authorization.....	24
4.3	Dependent System(s).....	25
4.4	Trouble Shooting	25
4.5	System Recovery	25
4.5.1	Restart after Non-Scheduled System Interruption	25
4.5.2	Restart after Database Restore	25
5.	Continuity of Operations	25
6.	Disaster Recovery.....	25
6.1	Required:	26
6.2	Assumptions:	26
6.3	Web/Apache server (Falling Waters):	26
6.4	WebLogic server (Falling Waters):	27
6.5	Database server (Falling Waters):	27
6.6	Database server (Hines):	29
6.7	Web/Apache server (Hines):	29
6.8	WebLogic server (Hines):	30

6.9	Load Balancer (Hines):	30
7.	System Support.....	32
7.1	Support Structure.....	32
7.1.1	Support Hierarchy	32
7.1.2	Division of Responsibilities	32
7.2	Support Procedures.....	33

1. Introduction

1.1 Summary

A Production Operations Manual (POM) defines the specific technical and operational processes that must be carried out on a daily, weekly, monthly, or yearly basis. A POM is an application/system-specific document containing detailed topology, dependencies, monitoring specifics, maintenance windows, etc. Additionally, it contains the system's scheduled events (regular production jobs, performance reporting, or maintenance windows, etc). The POM provides Field Operations staff the necessary instructions to operate and support production computer systems.

The production support for the System Name Production System is divided or shared between the Enterprise Operations & Infrastructure (EOI) and Product Development within the Office of Information & Technology (OI&T), and Corporate Data Center Operations (CDCO).

1.2 Purpose

The purpose of this document is to:

- Be used as a reference manual for the daily operation and maintenance of CISS/OHRS
- Assist support personnel on the resolution of system issues
- Assist in the capacity, maintenance, and upgrade planning of CISS/OHRS

1.3 Scope

The scope of this document is limited to CISS/OHRS. Any references to external systems is only for describing an interface and how the interface and the external system affects the operation of CISS/OHRS or as a tool that may be used as part of system monitoring or the support and issue resolution system.

1.4 Related Documents and Agreements

The VA Service Level Management Board (SLMB) has developed a memorandum that standardizes terminology and definitions for key documents used for implementation, operation, and monitoring of services provided by OI&T. The primary documents are Memorandum of Understanding (MOU), Service Level Agreement (SLA), Service Level Requirements (SLR), Operational Level Agreement (OLA), Operations and Maintenance (O&M), and Production Operations Manual (POM). The purpose and relationships of these documents are summarized below.

1.4.1 Memorandum of Understanding (MOU)

The Memorandum of Understanding (MOU), a written agreement between an OI&T service provider and customer(s), documents the services that each party will provide for a program or service. The MOU is the foundation document upon which the SLA, O&M Plan, and others are built. The MOU is a strategic document, whereas the SLA, O&M, and POM are more functional/tactical documents.

The MOU serves as the signatory document that invokes the SLA. The SLA/SLRs are referenced in the appendix of the MOU, allowing them to be managed or modified without renegotiating the entire MOU.

1.4.2 Service Level Agreement (SLA)

A Service Level Agreement (SLA) is a consolidated mutual agreement between a service provider and customer(s) that documents and describes agreed levels of performance and availability. The SLA describes Service Level Targets (SLTs), key performance indicators, monitoring approach, and a process for managing the service levels. In the VA, all SLAs are approved, negotiated, and governed through the Service Level Management Board (SLMB).

1.4.3 Service Level Requirements (SLR)

In the VA, Service Level Requirements (SLRs) are a list of basic performance measurement requirements. A SLR is proposed by the customer and negotiated with OI&T to reach a good faith agreement on the acceptable level of service and the metrics to monitor the service. The SLR is a service-specific breakdown (usually in a table) in an SLA appendix with a unique name and number.

After the SLR is negotiated, it results in an agreed Service Level Target (SLT) with metrics, measurement techniques, and assumptions. The SLA and SLTs are a combined document.

1.4.4 Operational Level Agreement (OLA)

An Operational Level Agreement (OLA) is an agreement between two or more OI&T entities that documents agreed service levels for general performance or critical services. An OLA is very similar to a SLA except that it is internal to OI&T functional units. An OLA defines specific key performance indicators and related metrics to measure success criteria. OLA metrics should form the foundation upon which SLA metrics can be derived for customer-facing services.

1.4.5 Operations and Maintenance Plan (O&M)

The Operations and Maintenance (O&M) Plan defines the operational support tasks and activities that each of the Office of Information & Technology (OI&T) functional areas are required to provide in the delivery and support of a production enterprise system. The O&M Plan defines specific roles and responsibilities of OI&T functional support teams to avoid confusion over which party is responsible for specific areas of process, tasks, or actions. The O&M plan supports the specific service levels for each activity as defined in the Service Level Agreement (SLA), describes how performance is measured, and identifies the responsible entities for each activity.

All key functions are assigned to one or more responsible parties and activities are clearly defined in order to maintain and support the applications and system components throughout its life cycle. These roles and responsibilities are displayed in a tabular RACI format at the end of each section of the plan to further define **R**esponsibility, **A**ccountability, **C**onsultation, and **I**nformation roles.

1.4.6 Underpinning Contract

Underpinning Contract is an agreement between an IT service provider and a third party, including vendors, that provides goods or services that support delivery of an IT service to a customer. It is developed either by the Program Office or OI&T, depending on ownership of the budget/funds

1.5 Section Summary

Section	Summary
1. Introduction	This section describes the scope and purpose of the document, along with other relevant documents.
2. System Business and Operational Description	This section provides the reader with a description of the system. It describes what the system does in the context of the VA.
3. Routine Operations	This section describes what is required of an operator/administrator or other non-business user to maintain the system at an operational and accessible state.
4. Exception Handling	This section gives an overview of how system problems are handled. It should describe the general expectations of how the administrator and other operations personnel should respond and handle system problems.
5. Continuity of Operations	This section describes the processes or procedures that operations personnel need to execute in order to fulfill their responsibility in the systems Continuity of Operations plan (COOP).
6. Disaster Recovery	This section describes the processes or procedures that operations personnel need to execute in order to fulfill their responsibility in the systems Disaster Recovery (DR) plan.
7 System Support	This section describes the VHA system support structure and how to use it to resolve system problems.

2. System Business and Operational Description

The Clinical Information Support System (CISS) project is a HealtheVet initiative from the Veterans Program portfolio. It is a Web-based portal application that provides a central interface for users to access information and applications necessary for their roles. The applications accessed through CISS are called partner systems. The initial CISS partner system is the Occupational Health Record-keeping System (OHRS), a Web-based application that enables occupational health staff to create, maintain, and monitor medical records for VA employees and generate national, VISN, and site-specific reports.

While implementing the CISS framework and the OHRS application, the CISS project team follows an agile software methodology to support rapid programming and short six-month releases to production. For more information please view the Agile Software Development Methodology and other documents available on the [CISS TSPR page](http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1256&Type=Active):

(<http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1256&Type=Active>).

This document contains instructions to help System Operators administrate and troubleshoot the delivered software. System Operators are defined as IT staff at the data centers where CISS is deployed.

2.1 Operational Priority and Service Level

The CISS project is a 24x7 system.

2.2 Logical System Description

Intranet access to the application is achieved from the customers' web browsers to a URL address associated with the Load Balancer's Virtual Server. Connectivity is directed to the CISS web servers, with the exception if requesting the Web-based content-sensitive help; all other traffic is redirected to the WebLogic application servers and their configured server ports. The CISS login portal webpage interacts with the VA Lightweight Directory Access Protocol (LDAP) service to determine access to the portal and any partner applications. Once access is gained and the OHRS partner application button is accessible, the OHRS application may be launched. OHRS application saves data into a local database and certain functions require interactions between the VistA systems of the chosen Site.

2.3 Physical System Description

The CISS servers consist of six physical servers, consisting of two Web servers, two Applications servers, and two Database servers. Redundancies are achieved through multiple methods: Replication of data at the OS and Application levels.

The architectural design of each of the three groups consists of different redundancies:

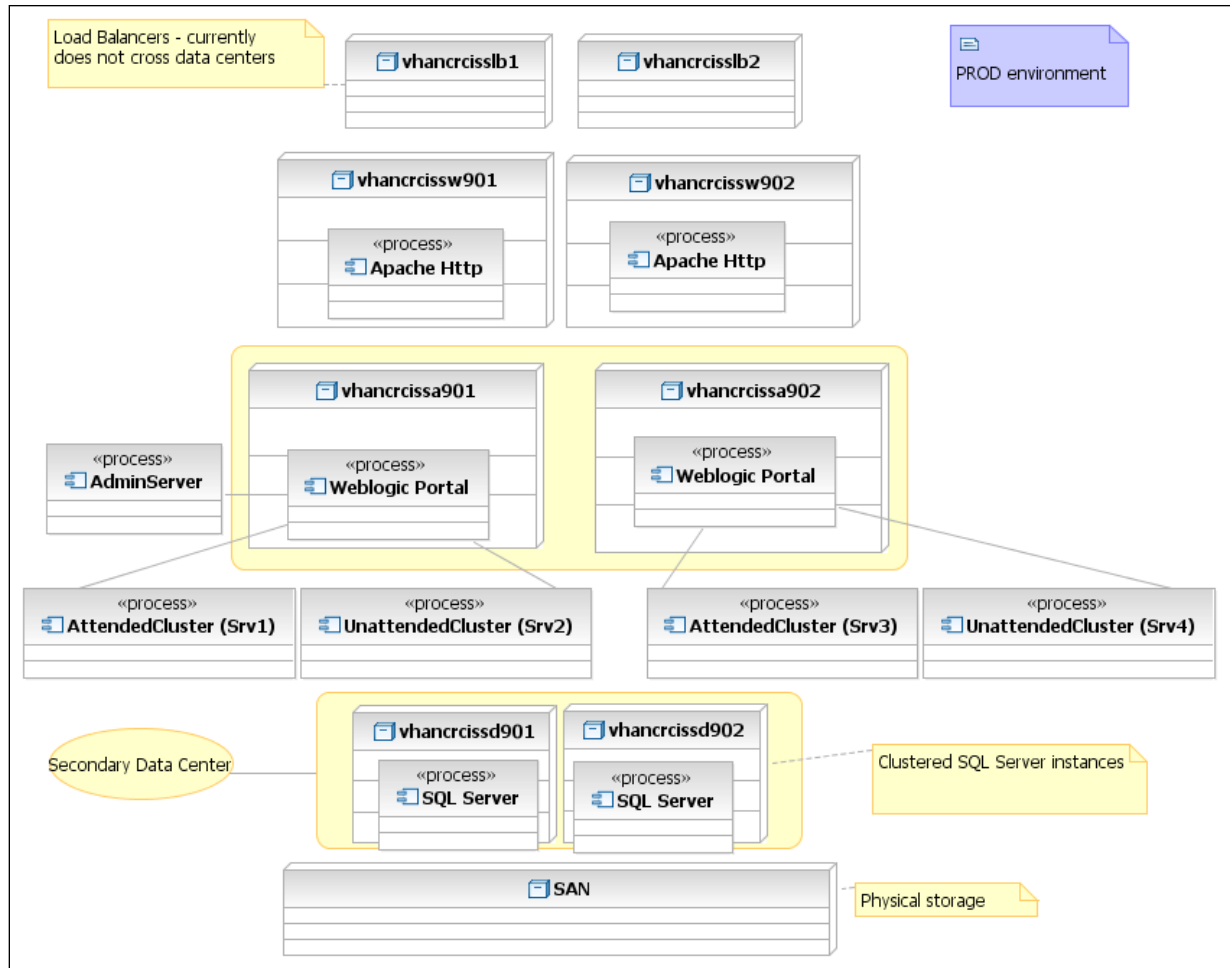
- The database servers are to be clustered at the OS level and at the database application level. The database servers are connected to a SAN, for additional storage, redundancy, and availability.
- The two web servers are designed to run exactly the same functionally, through non-clustered. OS level synchronization keeps the two servers consistent.
- The two application servers are not clustered at the OS level, but are clustered at the Application level. OS level synchronization and application implemented clustering maintain the redundancies.

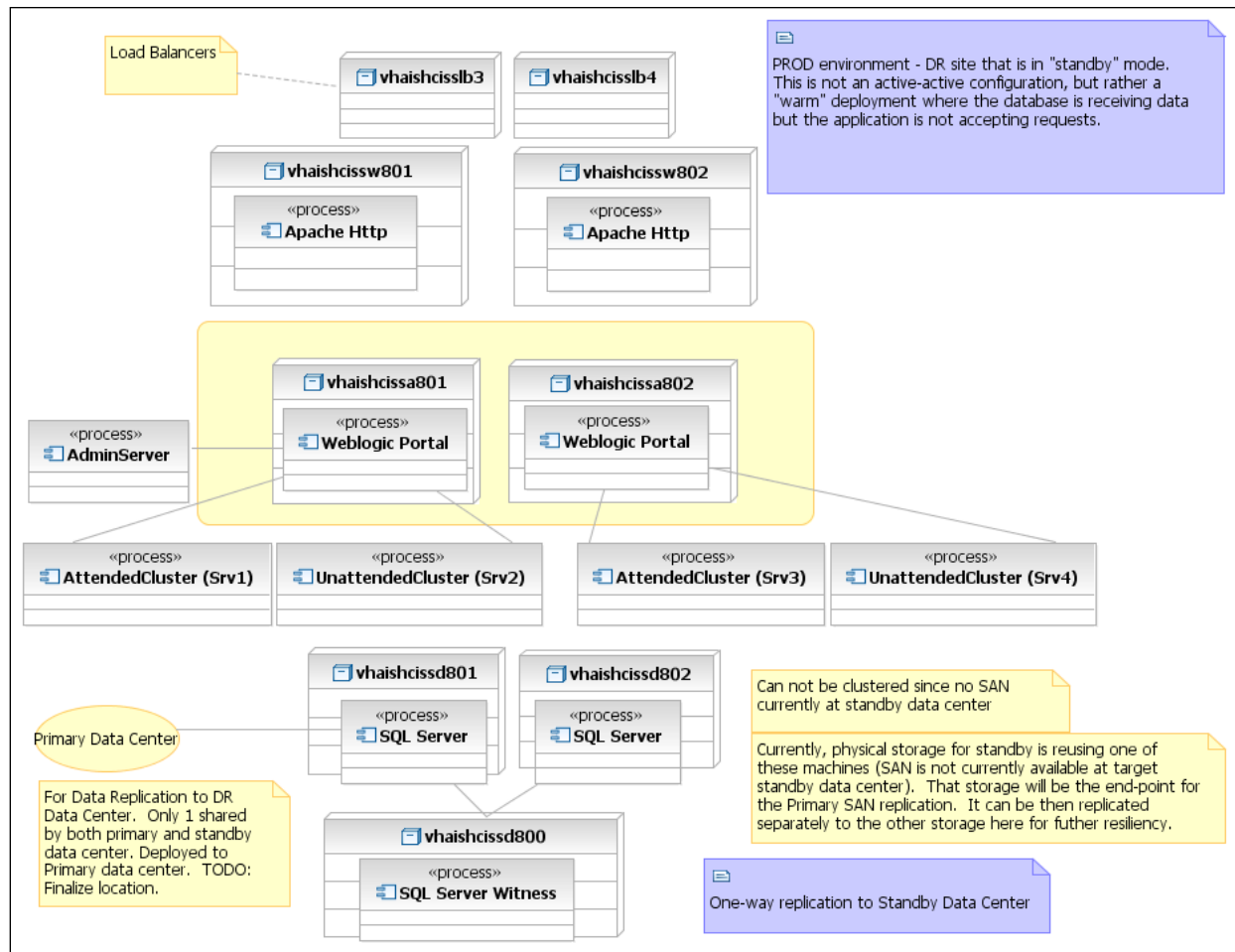
The Current systems implemented are HP ProLiant DL380 G5 servers, Intel ® Xeon ®CPU E5420 @ 2.50GHz 64 Bit Dual Quad core Processors, Dual Power Supplies, Dual Gigabit Network interfaces, iLO2 – Integrated Lights Out management port, RAID-controlled 6 HDD, 16 GB Memory. Microsoft Windows 2003 Enterprise and Red Hat Enterprise Linux 5.x are the Operating Systems of the systems. All Systems are attached to sites Gb network. ILO's have not yet been implemented; initially the Core switches did not have enough available ports.

Six of the Servers reside at Falling Waters, WV (CDCO), the Production site. Seven other Servers are located at Hines, IL. The Hines site is considered the Disaster Recovery (DR) site.

Main difference between the 2 data centers are:

The Hines, IL data center's initial implementation did not have the SAN storage available to attach to the database servers; the database servers alternative was to run using their local storage and leverage mirroring between the two database servers. Another difference is the additional MS Windows server as the MS SQLServer "Witness" server. The "Witness" server monitors the two Hines database servers, and delegates which server is the Primary and the other as the Stand-by nodes.





2.4 Software Description

- The Operating Systems:
- Microsoft Windows 2003 Enterprise Edition x_64 Bit

Red Hat Enterprise Linux 5 x_64 Bit

The Applications:

- BEA / Oracle WebLogic 10.3.2
- Microsoft SQLServer 2005
- Apache 2.2.3
- VistALink 1.5

File system sizes differentiate between the Servers Functions:

- Windows servers Database servers

- Local Drives
 - C: 40 GB
 - D: 96 GB
 - E: 292 GB
 - F: 254 GB
- SAN Attached (If attached, and if the Active server in the Cluster)
 - G: 102 GB
 - H: 102 GB
 - J: 102 GB
 - L: 34 GB
 - M: 17 GB
 - O: 85 GB
 - Q: 500 MB
- RHEL Application server
 - /dev/mapper/rootvg-root 992M /
 - /dev/mapper/rootvg-opt 3.9G /opt
 - /dev/mapper/rootvg-var 3.9G /var
 - /dev/mapper/rootvg-tmp 3.9G /tmp
 - /dev/mapper/rootvg-usr 3.9G /usr
 - /dev/mapper/rootvg-home 2.0G /home
 - /dev/cciss/c0d0p1 251M /boot
 - tmpfs 7.9G /dev/shm
 - /dev/mapper/rootvg-u01 97G /u01
 - /dev/mapper/rootvg-u02 9.9G /u02
 - /dev/mapper/rootvg-u03 9.9G /u03
 - /dev/mapper/rootvg-u04 9.9G /u04

Example: Mounted Network File Share Listed Below:

- vhancrcissw901:/u02/PAID 20G /u02/PAID
- vhancrcissw901:/u02/PATIENTIMPORT 20G /u02/PATIENTIMPORT

There are numerous scripts involved in monitoring and synchronizing of servers systems.

2.4.1 Background Processes

The Microsoft SQLServer runs a Daily “Maintenance Plan”:

- Maintenance Clean up on Local server connection Clean up Database Backup files
- Clean up history on Local server connection History type: Backup, Job, Maintenance Plan
- Backup Database on Local server connection: CISS, Model Databases - Transaction Logs
- Check Database integrity on Local server connection: CISS, CISS_distributor, master, model, msdb
- Update Statistics on Local server connection: CISS, CISS_distributor, master, model, msdb

- Backup Database on Local server connection: CISS,CISS_distributor,master,model,msdb
- Reorganize index on Local server connection: CISS Tables

The SQL backups are stored on the mapped H: SAN attached drive. The database servers have OS level backup run at 5:00 A.M. every day. The DOS batch script does a checksum of the last backups, XCOPY of the files to the DR servers, purges any files that are over five days.

The Linux servers, application, and web servers each have scheduled jobs:

The web servers monitor any PAID files that arrive and rename the file with a Date/Time stamp. If processed files are found, after OHRS has uploaded the PAID content into the OHRS database, the files are TAR GZIP'd into an archive file.

Example Crontab:

```
#*      *      *      *      *      [command to be executed]
#-      -      -      -      -
#|      |      |      |      |
#|      |      |      |      +----- day of week (0 - 6) (Sunday=0)
#|      |      |      +----- month (1 - 12)
#|      |      +----- day of month (1 - 31)
#|      +----- hour (0 - 23)
#+----- min (0 - 59)
*/10 *      *      *      *      *      /bin/bash /usr/local/bin/cissPAID_update_filename.bsh
```

Also the Web servers monitor, Similar Process with VAADERS data.

(Scripts / Process still pending)

2.4.2 Job Schedules – (Reference Background Processes)

UNDERLINED TEXT is the User and its entries

```
#####

###   The Following is a Description on the Crontab syntax   ###

#####

#*      *      *      *      *      command to be executed
#-      -      -      -      -
#|      |      |      |      |
#|      |      |      |      +----- day of week (0 - 6) (Sunday=0)
#|      |      |      +----- month (1 - 12)
#|      |      +----- day of month (1 - 31)
#|      +----- hour (0 - 23)
#+----- min (0 - 59)
```

ROOT -- Webservers

```
### Setting up for later the retrieval of new Files
```

```
#3      8,10,12,14,16,18 *      *      1,2,3,4,5      bash
/usr/local/bin/OFA_sftp_retrieve.bsh
```

```
### For OFA samba share with samba_up.html
```

```
*/1      5-22      *      *      *      /bin/bash /var/www/cgi-bin/SAMBA_update.bsh -C
1      0      *      *      *      /bin/bash /var/www/cgi-bin/SAMBA_update.bsh -R
```

PBM -- Webservers

```
*/10      *      *      *      *      /bin/bash /home/pbm/.bin/rsync.bsh
```

Weblogic

```
2      7      *      *      *      /bin/bash
/u01/app/bean/weblogic/domains/CISSDomain_Prod/bin/check_vlj_connectors.bsh

1      4      *      *      0,3      /bin/bash /usr/local/bin/CG_Prod.bsh -E PRD

*/4      *      *      *      *      ~/weblogic/common/bin/wlst.sh
/usr/local/etc/Connections.py ~/ciiss.properties >/dev/null 2>&1

2      7      *      *      *      ~/weblogic/common/bin/wlst.sh
/u01/app/bean/weblogic/domains/CISSDomain_Prod/WLST_scripts/vljMonitor.py
ciiss.properties ALL
```

2.5 Dependent Systems

Systems on which CISS/OHRS are dependant:

- VistALink connectivity to each VA VistA system
- Personnel and Accounting Integrated Data System (PAID) -- Receive automated uploaded files
- VAADERS – Receive manually uploaded files
- Other Federal Agencies (OFA) – This Process has been put on hold.
- Standard Data Service (SDS)

3. Routine Operations

Using Linux bash scripts to extract data from the different servers and systems, the data is gathered, parsed, and output in csv, xml, flat file, or direct to the email. The systems administrator will monitor the WebLogic JVM - Java Virtual Machine Memory, File System usages, VistALink Adaptor connectivity via Dashboards, Consoles, or received emails. The systems administrator will also deploy the new artifacts during planned outages, stop and start the WebLogic managed servers, monitor system backups. Routine OS patches, updates will be performed via mechanisms standard to the OS.

The database administrator will monitor database growth, replication, and backups. The database administrator will perform updates, upgrades, and maintenance to the database or database engine.

3.1 Administrative Procedures

3.1.1 System Start-up

3.1.1.1 Windows Database Server

- Once the server is powered on, the SQLServer database instance for CISS will automatically start. To verify service is running, open the Windows 'Services,' locate the following:
 - SQL Server (PROD_SQLSERVER)
 - SQL Server Agent (PROD_SQLSERVER)
 - SQL Server Browser
 - SQL Server FullText Search (PROD_SQLSERVER)
 - SQL Server Integration Services
 - SQL Server VSS Writer
- Log into SQL Server Management Studio to confirm SQL server database is up and running and that you can connect to the database.
- The 5:00 A.M. backup is an OS level scheduled task.

3.1.1.2 Linux Web server:

- Once the server is Powered on, check the Network File Share (nfs) and Apache web services (httpd), and Very Secure File Transfer Protocol (vsftpd) services are running:

- Sudo to the Root (Super User):
`sudo su -`
- Check that the nfs service is Running:
`service nfs status;`

If Not running, start the service:

```
service nfs start;  
  
chkconfig --level 234 nfs on;
```

- Check that the httpd is running
`service httpd status;`

If Not running, start the service:

```
o service httpd start;  
o chkconfig --level 234 httpd on;
```

- Check that the vsftpd is running
`service vsftpd status;`

If Not running, start the service:

- o `service vsftpd start;`
- o `chkconfig --level 234 vsftpd on;`

3.1.1.3 Linux Application server:

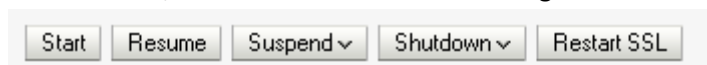
- Once the server is powered on, the WebLogic Node manager must be started.
 - o Sudo to the weblogic user:
`sudo su - weblogic3 ;`
 - o Start the nodemanager and background the Process:
`bash nodemanager/startNodemanager.sh &`
 - o Allow the nodemanager to start, check by verify the port 5556 is listening, run the lsof command:
`/usr/sbin/lsof -Pni |grep weblogic | grep LISTEN ;`
- Start the WebLogic Administrative Console:
 - o `bash CISSDomain/startWeblogic.sh &`
 - o Watch for the following text in the output sent to the screen.
 - `<Server state changed to STARTING>`
 - `<Server started in RUNNING mode>`
 - o Verify the Admin server started by either the following methods:
 - Opening a web browser to the `http://vaww.ciss.med.va.gov/console`
 - Run the `getstatus.sh` script:
 - `cd ${HOME};`
 - `getstatus.sh ciss.properties ;`
 - Run the lsof command Looking for the Admin server port 7100:
- Start the WebLogic managed servers using 1 of 2 methods:
 - o Command Line:
 - `cd ${HOME};`
 - `startservers.sh ciss.properties ALL ;`
 - `getstatus.sh ciss.properties ;`
 - o Via the Admin console:
Log into the Admin console using the host name and admin port for the URL:

Example: <http://vhancrcissa901:7100/console>

- Select the Control tab
- Select the Check box next to the managed servers (Srv1, Srv2, ...)

<input type="checkbox"/>	Server
<input type="checkbox"/>	AdminSrv_Maint(admin)
<input checked="" type="checkbox"/>	Srv1
<input checked="" type="checkbox"/>	Srv2

- Click the 'Start' Button, located above the list of managed servers.



Note: Start time takes roughly 15 minutes.

- Press F5 to refresh or click the button with the curved circular arrows, to check the Status
- Verify the Apache is running:
 - `ps -ef | grep httpd;`
 - You should find multiple instances.
 - If no instances are found, you must be root to start the service.
 - `service httpd start ;`
- Verify that the NFS is started:
 - Sudo to the Root (Super User)
 - `sudo su -`
 - Check the nfs service is Running
 - `service nfs status;`

If not running, start the service:

 - `service nfs start;`
 - `chkconfig --level 234 nfs on;`
- Verify all Mount Points are Connected:
 - As the Root User:
 - `mount -a;`

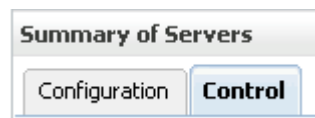
3.1.2 System Shut-down

The best solution to bringing the servers offline is as follows:

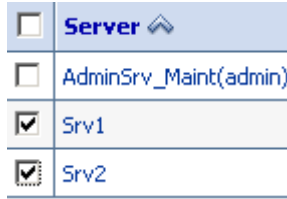
- Either via command line or console, stop the WebLogic managed servers
 - Login to the WebLogic Admin node server via ssh
 - `sudo su - weblogic3 ;`
 - `cd ${HOME};`
 - `stopservers.sh ciiss.properties ;`
 - `getstatus.sh ciiss.properties ;`
 - `ps -ef |grep '[Aa]dminSrv'|awk '{print $1}' |xargs -i kill {};`
 - Login to the WebLogic Admin console
 - Navigate to the Summary of Servers



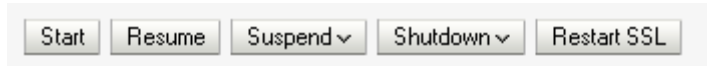
- Select the 'Control' Tab



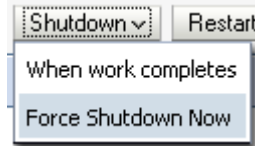
- Select all applicable manage servers check boxes



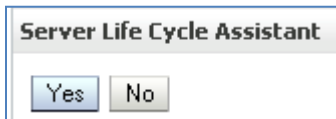
- Click the 'Shutdown' menu button,



- Select 'Force Shutdown Now' from the drop-down selection.



- Select the 'Yes' Button to shutdown the managed servers selected.



- If Admin servers was not selected, repeat three previous steps to shutdown the WebLogic Admin server.
- Shutdown the Linux server OS.

- Both application and web server can be shutdown

- Sudo to the Root user.
 - `sudo su - root ;`

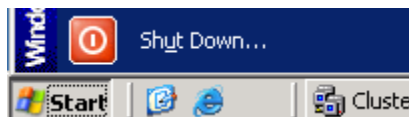
WARNING: running the next command will HALT the server, unless the ILO access has been configured or there is a physical person to power on the server:

```
shutdown -h now.
```

- Shutdown Windows server OS

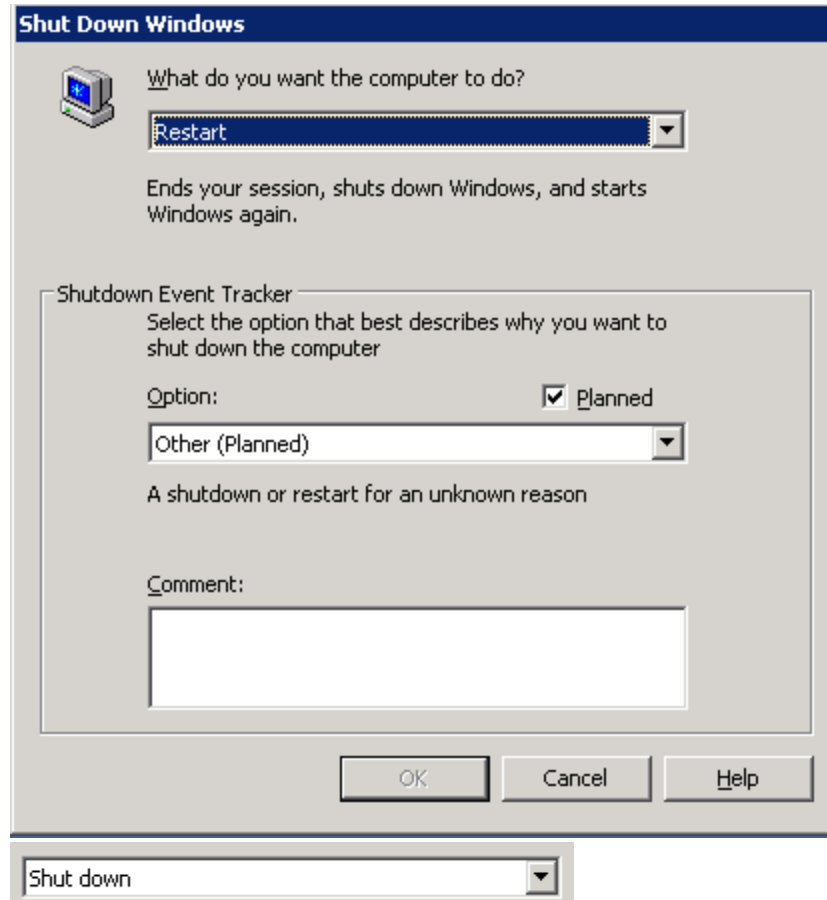
- The SQLServer Database engine and any other processes will be brought down normally thru the system services.

- Shutdown Windows server
- Click the **Start** button

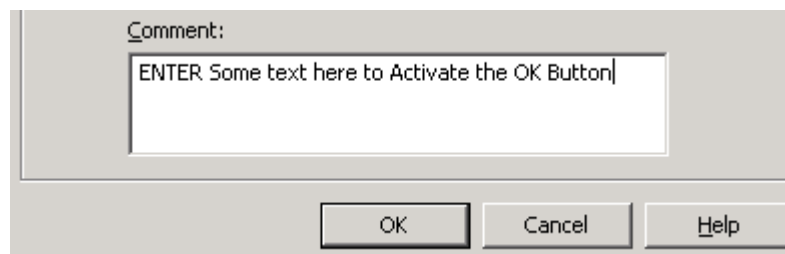


WARNING: running the next set of screen will HALT the server, unless the ILO access has been configured or there is a physical person to power on the server.

- Change the Dropdown box from **Restart** to **Shut down**:



- Enter some Reason or Comment for shutting down the server.



- Click **OK**.



3.1.3 Back-up and Restore

The Production Database is the only instance in the CISS/OHRS environment where an official backup is being handled. The SQLServe Database has its own mechanism for database backup and restore:

- Database backup procedures: (see Section 3.1.3.1)
- Database restore procedures: (see Section 3.1.3.2)

3.1.3.1 Back-up Procedures

- Database
 - Database Administrator can elaborate. The internal backup schedule backs up the Transactional log and all databases, each exported to their own separate directories and corresponding database names.
 - Two nightly backups are performed
 - 9:00 P.M. -- mostly for the previous day's transactions
 - 4:00 A.M.
- SAN Device
 - Every evening full back ups are run at 6:00 P.M. and the following directories are being backed up to tape (mentioned in the section Storage and Rotation).

3.1.3.2 Restore Procedures

- SAN Device
 - Daily Linear Tape-Open (LTO) tapes are stored locally at the site.
 - An official request must be made to the EMC staff to restore data from tape and an alternate location must be established to restore the file(s).
- Database
 - A full database backup is performed each morning at 4:00 A.M. immediately followed by a Transaction Log backup. The same process is repeated at 9:00 P.M. The backup files are stored on a drive that is distinct from the database files. The database files are archived on to the disaster recovery server, and the storage area network engineers perform server level backups that send the files to a secure off-site facility. The backup and recovery policy used for the OHRS database is through SQL Server Maintenance Plan backups. Recovery is achieved by using SQL Server Enterprise manager, selecting “Restore Database” under database tasks and selecting the latest backup and transaction log file.

3.1.3.3 Back-up Testing

Not applicable

3.1.3.4 Storage and Rotation

- Use EMC NetWorker 7.6 as the backup application/system to back up all hosts in Falling Waters (FW) and Hines to tape.
- Both FW and Hines also use new Quantum i6000 tape libraries as our tape backup systems. Each of these new tape library units provide six Linear Tape-Open (LTO)-4 tape drive systems to backup data to tape (LTO-4 tapes will support 800GB native/1600GB compressed of data).
- Backups are performed daily/nightly via the network for most systems.
- Times in which backups are performed are based on the requirements and input of the corresponding project owner, Database Administrator (DBA), application owners, etc.
- Type of backups performed are weekly full and daily incremental.
- EMC staff performs a monthly backup which is retained per VA long-term retention policies.
- Tape rotation: all short-term retention tape backups (90 days or less) rotate based on the need and when tapes have expired.
- All short-term retention tape backups are temporarily stored in a secure location onsite (once the tapes have been ejected from the tape library) until they have expired and can be recycled/reused.

- All long-term retention tape backups are stored at a secure offsite facility (Iron Mountain). They will usually do one scheduled pick up per week – tapes are shipped offsite on a routine basis using this system.
- Retention is based solely on the requirements of the specific project – the standard for the retention of all backup data is 90 days, and then the tapes are recycled. Monthly backups are retained for two years (at Iron Mountain) under the current standard VA retention policy (mentioned above).

3.2 Security / Identity Management

CISS/OHRS has many levels of security, starting at the OS layer, to the application portal, database, CISS, and OHRS applications. Each section below will have different methods or levels of complexity.

3.2.1 Identity Management

- OS:

Users are identified by their roles in the project, by the VA and contracting staff. Roles and permissions are determined by the Systems Admin and Database Admin, and are communicated to the team.

- WebLogic:

User requests access to the WebLogic application from the Systems Administrator. The SA determines access needs, and reviews alternate means of access to assist the user's request. If console access is required, READ-ONLY/MONITOR user access is given to the request, unless more access is necessary.

- Portal:

Users request access from their local occupation administrative staff and the request is communicated to the VA PM for approval. The VA PM will grant the user access using LDAP to associate the users VA ID with the CISS/OHRS LDAP organizational unit (OU).

- OHRS application:

User portal access establishes the user's roles and privileges and options usability within the OHRS application.

3.2.2 Access control

- OS:
 - Users are identified by their role in the project or dependency, and granted the minimum access to achieve their task or role.
 - Using their VA issued log in as their account,
 - The account is created with details of the person's name and title.
 - Specific rights are given to the user's log in, and any additional sudo (Linux) rights and privileges are configured.
 - (Linux) The amount of time the user requires access determines their account expiration

- WebLogic:

User is added via the Console

- Password and roles assigned.

- Portal:

All users can access the portal using their VA user ID and password.

- OHRS:

- Only the USER ID associated with the OHRS portal will be granted to the 'OHRS' Button to access the OHRS application.
- Each person is granted a role or set of roles in the OHRS application, and depending on the role, each person has access to different aspects to the OHRS application and permission to execute different tasks within the application.

3.3 User Notifications

The Systems Administrator or Database Administrator informs the project team of a request for an outage window. The project team requests, via daily meetings and/or email, from the VA systems Owner (VA PM), permission for a scheduled outage window. The VA PM notifies the User Community of the Outage and its implications.

3.4 System Monitoring, Reporting & Tools

- OS

- The Linux servers have standard monitoring scripts that send emails to the root user. Those standard scripts, in conjunction to Multi Traffic Router Graph (MRTG), and some custom script inform the Systems Administrator and the Database Administrator of any issues or pending issues.
- No tool can monitor every aspect, so custom scripts are created to run against Windows, Linux SNMP, and the WebLogic Scripting Tool (WLST).
- MRTG is used for its ability to chart any numerical data and has other underlying abilities.
- Using PHP, WLST, MRTG, custom scripts, and system generated emails, the Systems Administrator has a wealth of options and avenues of monitoring the systems.

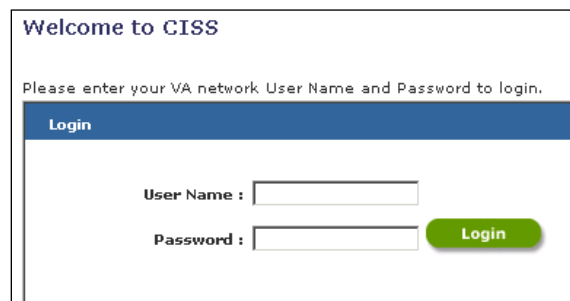
- Database Administration :

- The Microsoft SQLServer has some internal Reporting and Monitoring capabilities.
- Emails are sent to the Systems Admin and Database Admin for the nightly backups.
- The Replication manager tool within the Enterprise Studio is used in order to monitor the performance of replication between the CISS-OHRS server and DR servers.

3.4.1 Availability Monitoring

Availability of the CISS/OHRS application:

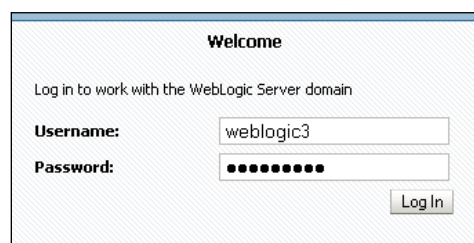
- Launch a browser to the application URL,
 - The traffic will pass through the Load Balancer to the Apache servers.
 - The WebLogic plug-in will validate the connectivity to the WebLogic-managed server located on the Application server,.
 - If the application is available, the network traffic is passed to the WebLogic-managed server.



- If failure, the traffic is re-directed to a static Error/Maintenance webpage.



- WebLogic Administration Console
 - Log into the Admin console:



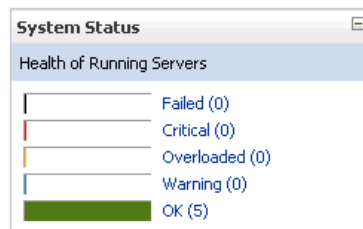
- Navigate to the Deployments page.



- Review the Deployed Applications for any potential Issues, Warning:

<input type="checkbox"/>	Name	State	Health	T
<input type="checkbox"/>	ciss	Active	Warning	Ei A
<input type="checkbox"/>	ohrs	Active	OK	Ei A
<input type="checkbox"/>	vlj283	Installed		R
<input type="checkbox"/>	vlj358	Active	OK	R

- Review the Health of the Running Managed servers:



3.4.2 Performance/Capacity Monitoring

- Using the MRTG application, systems can be monitored for performance and capacity using the data captured. MRTG charts assist the DBA and SA in their overall analysis of the capacity and recommendations accordingly.
 - Server network bandwidth, speed, usage.
 - WebLogic: Java Virtual Memory (JVM) heap sizes, and usage
 - File System: size, usage, Input/output
 - System uptime, system or IO wait, usage
- Data can be analyzed actively, 'On demand', or post event. Each is made available via different means.

3.4.3 Critical Metrics

- Additional Metrics need to be indentified for future monitoring
- Hard disk drive (HDD) usage
- Network usage
- Input/Output (I/O) to the HDD
- WebLogic can monitor JMS messaging and the Console can show problems. The need for monitoring this has been very minimal; no further action has been requested.

3.5 Routine Updates, Extracts and Purges

- Database
 - DBA to expand on updates , extracts, and any purges
 - SDS update
 - An Email is sent to all projects that officially use the SDS database.
 - A manual update is done by the Database Administrator and requires the OHRS application to be recycled. This allows clean connections to the updated data.
 - PAID Data
 - PAID data is uploaded to the Web server's VSFTP service
 - The updates are automated at the source, and can be uploaded multiple times a day.
 - A Linux cron job executes a custom script to check for any new files and rename the uploaded DATA.PAID files to the {Time stamp of when the file was created}.PAID.
 - This custom script also initiates a Re-sync to all of the Production and DR web servers.
 - Twice a month, the OHRS application internal job loads sequentially all *.PAID files, renaming the files {Time stamp of Processed}.PAID.{Time processed by OHRS app}.processed
 - MD5 Checksum of the processed files are recorded to a MD5 file.
 - TAR and GZIP the processed files.
 - GZIP file is tested for validity
 - A final MD5 checksum is performed on the final files before removing the uncompressed processed files.

- Database extracts are performed periodically for use in the PROD Mirror and SQA testing Databases. DBA to expand.

3.6 Scheduled Maintenance

Every three months, all OS patches and updates are performed using Development Lifecycle procedures.

3.7 Capacity Planning

Once a year the SA, DBA, and Project team will sit down and review the capacity and performance of the previous year, noting any potential areas of interest, and making any recommendation and adjustments. From this meeting, a plan of action will be scheduled and any outage requests sent to the VA PM.

4. Exception Handling

4.1 Routine Errors

Like most systems, System Name may generate a small set of errors that may be considered “routine.” These errors are routine in the sense that they have minimal impact on the user and do not compromise the operational state of the system. Most of the errors are transient in nature and only require the user to retry an operation. The following sub-sections describe these errors, their causes, and what, if any, response an operator needs to take.

While the occasional occurrence of these errors may be routine, getting a large number of an individual error over a short period of time is an indication of a more serious problem. In that case, the error needs to be treated as an exceptional condition.

4.1.1 Security

- Reverse mapping checking getaddrinfo for xxxx-lt.vha.med.va.gov failed - POSSIBLE BREAK-IN ATTEMPT!
 - This error is normal because of the slowness of the VPN DNS updates.
 - A user connects via VPN into the VA network and the DNS system should be updated with the connecting Workstation/Laptop hostname are associated with the IP address. The DNS is slow to propagate the changes across the VA network. When the Linux server does a reverse lookup of the requesting IP, the discrepancy of Hostnames occurs.

4.1.2 Time-outs

- Each user has a 15-minute inactive timer on the Linux servers. Once the time has expired, their current session is logged out.
- VistAlink Adapters have timeouts, while attempting to connect to the configured Port and IP for the associated Station ID.

4.1.3 Concurrency

Not applicable

4.2 Significant Errors

Significant errors can be defined as errors or conditions that affect the system stability, availability, performance or otherwise make the system unavailable to its user base. The following sub-sections contain information to aid administrators, operators, and other support personnel in the resolution of errors, conditions, or other issues.

- File system full errors
- Application Errors, related to Database Connection, JVM sizes, and deployable artifact problems.

4.2.1 Application Error Logs

- Apache
 - All Apache logs are written to the directory `/var/log/httpd/`, unless specially identified in the Apache configuration files.
- Security / SSH
 - `/var/log/secure`
- General Messages
 - `/var/log/messages`
- WebLogic Managed servers
 - `{DOMAIN Home}/servers/{MANAGED server}/logs/`

4.2.2 Application Error Codes and Descriptions

Not applicable

4.2.3 Infrastructure Errors

4.2.3.1 Database

- One error situation with SQL Server databases, which is encountered sometimes in situations where a DBA has not been continuously hands-on monitoring the database, occurs when the size of the Transaction Log file grows so large that there is a danger of running out of disk space. This is a serious issue. Normally, the size of the database files needs to be monitored such that this situation will not occur.
- The correct way to control the growth of the Transaction Log file is to regularly perform a full database backup and IMMEDIATELY follow it with a Transaction Log backup. This process may even be back-to-back repeated one time; this should shrink the size of the Transaction Log.

- Note however, in a replicated scenario like OHRS, if the replication queue is broken, then the transaction log grows in size, and it does not shrink even with the backup. In this case, the replication needs to be restored first so that the queues get flushed.
- A rarely encountered but serious error situation happens if the SQL Server database were to ever go into suspect status. In this situation, the only way to recover would be to have the latest database and transaction log files available, and run the following steps one at a time:
 - EXEC sp_resetstatus 'CISS';
 - ALTER DATABASE CISS SET EMERGENCY;
 - DBCC checkdb('CISS');
 - ALTER DATABASE CISS SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
 - DBCC CheckDB ('CISS', REPAIR_ALLOW_DATA_LOSS);
 - ALTER DATABASE CISS SET MULTI_USER;

4.2.3.2 Web Server

- Most errors are syntax errors after modifying the configuration files; check syntax and verify against another Apache configuration file.

4.2.3.3 Application Server

- VistAlink errors:
 - Root cause
exception:gov.va.med.vistalink.security.m.SecurityTooManyInvalidLoginAttemptsFaultException:Fault Code: 'Server'; Fault String: 'Logon Failed'; Fault Actor: ";Code: '183005'; Type: "; Message: 'Logon failure: 'Device/IP address is locked due to too many invalid signon attempts.'">
 - ResourceAllocationException thrown by resource adapter on call to ManagedConnectionFactory.createManagedConnection():
"gov.va.med.vistalink.adapter.cci.VistaLinkResourceException: Can not create VistaSocketConnection; Root cause exception: gov.va.med.net.VistaSocketException: Can not create TCP/IP socket.; Root cause exception: java.net.ConnectException: Connection refused ">

4.2.3.4 Network

Network failures are reported in numerous locations: the DMESG system, /var/log/messages, the application logs, and the WebLogic-managed server's logs. The nature of the problem determines where the error will be reported.

4.2.3.5 Authentication & Authorization

- Errors of authentication could be reported in the associated logs.

- Linux

The /var/log/secure files will report any issues connecting and authenticating the user.

- Samba

/var/log/samba/ smbd.log file will report any issues of authentication of connectivity issues.

- VSFTP

/var/log/vsftp.log file will report any errors connecting the VSFTP service.

- WebLogic Administration console

{DOMAIN Home}/servers/{Admin server}/logs/{ {Admin server}.log

4.3 Dependent System(s)

Not applicable

4.4 Trouble Shooting

Not applicable

4.5 System Recovery

The following sub-sections define the process and procedures necessary to restore the system to a fully operational state after a service interruption. Each of the sub-sections starts at a specific system state and ends up with a fully operational system.

4.5.1 Restart after Non-Scheduled System Interruption

- Use Section 3.1.1, for the actual details
- Verify database servers are started, and database is running.
- Verify web server is started, NFS is running, Apache is running.
- Verify application server is started, NFS mounted to web server, start weblogic admin application server, start managed servers.

4.5.2 Restart after Database Restore

Follow Section 6 - Disaster Recovery.

5. Continuity of Operations

Not applicable

6. Disaster Recovery

DR is a manual process

6.1 Required:

Access to Falling Waters and Hines via the following servers:

- WebLogic Admin server
- Apache Web server
- SQL Database server

6.2 Assumptions:

Production environment, passwords, SQL server DBA skills, RHEL / MS Windows 2003 SA skills, proper user level permissions, all servers are running at proper/normal runtime levels.

These procedures assume that the fail-over is planned and all sites are operational. They do not discuss returning to normal operations, which could be done by executing the same procedures again with Hines as the initial site and Falling Waters as the destination.

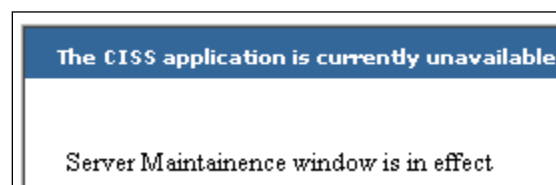
If the primary data center is down, you will need to rely on the replicated database at the DR site.

6.3 Web/Apache server (Falling Waters):

- Log into both web servers
- Sudo to the root user:
`sudo su - ;`
- Modify the `/etc/httpd/conf.d/weblogic.conf` file
 - Remove the # from the following line:

`# SetEnvIf Host vaww-prdadm.ciss.med.va.gov v_OK`
 - Insert a # in the line below:

`SetEnvIf Host vhancrcissw901 v_OK`
- Restart the Apache daemon:
`service httpd restart ;`
- Validate that the front door is closed:
`https://vaww.ciss.med.va.gov/ciss/`
- Should see the Following:



Rolling text:

Server Maintenance

Rolling text:

Click [HERE](#) to try again

- Validate that the Side door is open:
<https://vaww-prdadm.ciss.med.va.gov/ciss/>

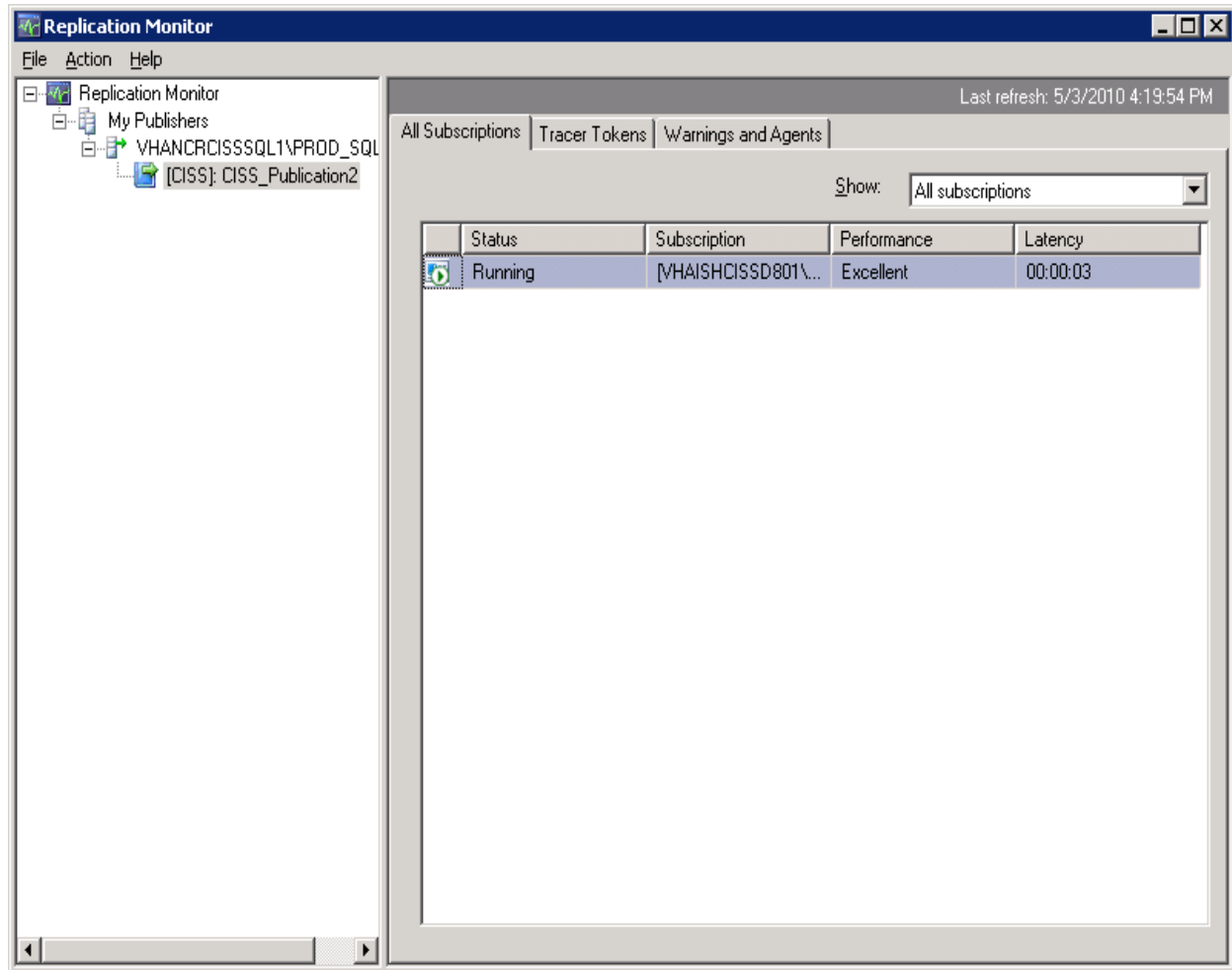
Note: this link is only valid after following the instructions above.

6.4 WebLogic server (Falling Waters):

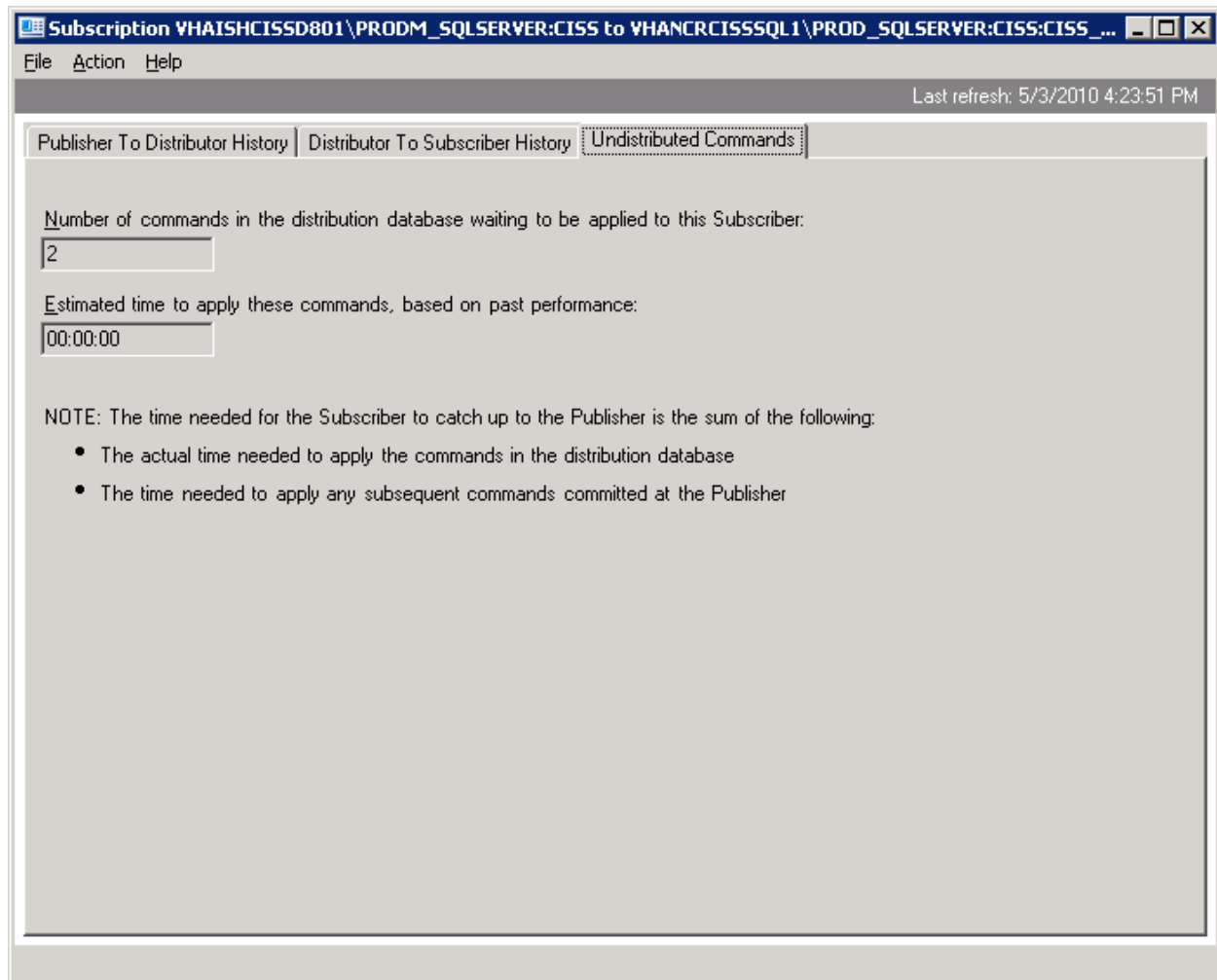
- Log into the node of the WebLogic application server.
- Check the Status of the WebLogic system:
 - Command Line:
 - Sudo to the weblogic3 user:
`sudo su - weblogic3 ;`
 - Run the following:
 - `cd ;`
 - `getstatus.sh ciss.properties;`
- Shutdown the managed servers
 - `cd;`
 - `stopservers.sh ciss.properties ALL;`
If servers will not stop/die, kill the PID of the Managed servers
 - `ps -ef|grep [Ss]rv |awk '{print $2}'|xargs -i kill -9 {}`

6.5 Database server (Falling Waters):

- Log into the Primary Windows SQL server machine.
- Make sure that DB is running and that there are no transactions happening.
 - Start -> All Programs -> Microsoft SQL Server 2005 -> SQL Server Management Studio using the SYSTEM user.
 - Right click Replication -> Launch Replication Monitor



- Double-click the Subscription name in the right-side window.
- Click on **Undistributed Commands** – the number of commands waiting should be zero. If it is not zero, press F5 to refresh screen until it is zero.



- Stop replication by running script Dropreplication.sql stored in the ClearCase stream Dev_OHRS_Data_mgt in the OHRS_db\Production Maintenance\Replication vobs.
- Make sure the application is disconnected from the database and make a backup of the CISS database.
 - Zip/WinRAR the Database backup and XCOPY to Hines.

6.6 Database server (Hines):

- Log into the Primary Windows SQL server machine.
- Make sure that DB is running and that there are no transactions happening.
 - Unzip/WinRAR - the Falling Waters Backup.
 - Restore the Falling Waters backup to CISS database.
 - Confirm Users can connect to the Database.

6.7 Web/Apache server (Hines):

- Verify that Apache is running.
 - Sudo to the root user
 - `sudo su - ;`
 - `service httpd status ;`

6.8 WebLogic server (Hines):

- Log into the node of the WebLogic application server.
 - Once given the “GO” from the DBA
- Start the weblogic managed servers:
 - Command Line:
 - Sudo to the weblogic3 user
`sudo su - weblogic3 ;`
 - Start ALL the Managed servers
`startserver.sh ciiss.properties ALL;`
- Verify that the WebLogic is running:
<http://vaww-dr.ciiss.med.va.gov/>

Note: this link is only valid after following the instructions above.

- Have testers smoke test the system

6.9 Load Balancer (Hines):

- Log into <http://10.3.29.103/>.
- Select “hines”



- Change weight from 0 to 100

A screenshot of a configuration window with two tabs: 'General' (selected) and 'Reso'. Under the 'General' tab, there is a section titled 'Site Configuration'. It contains four fields: 'ip' with a value of '10.3', 'agent' with a value of '10.3', 'weight' with a value of '0', and 'default site' with a checked checkbox.

- Click **Commit**:

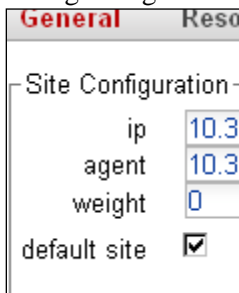


If grayed out (like above), you must contact the Load Balancer Administrator to grant you more permissions.

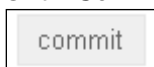
- Select “fw”



- Change weight from 100 to 0



- Click **Commit**:

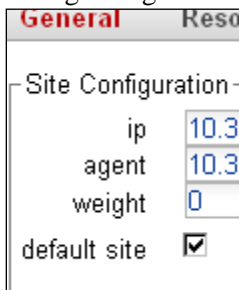


IF grayed out (like above), you must contact Load Balancer Administrator to grant you more permissions.

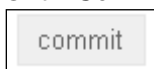
- Select “fw2”



- Change weight from 100 to 0



- Click **Commit**:



If grayed out (like above), you must contact the Load Balancer Administrator to grant you more permissions.

- Verify that the normal front door is accessible
 - <http://vaww.ciss.med.va.gov/>

7. System Support

An understanding of how System Name is supported by various organizations within the VA is important to operators and administrators of the system. In the event that you are unable to resolve an issue, then it is necessary to understand how to obtain support through OI&T's system support organizations. The following sections describe the support structure and provide procedures on how to obtain support.

The information in these sub-sections is a summary of parts of the CISS/OHRS O&M plan. This document is available in ClearCase and should be used if additional information is required.

7.1 Support Structure

This section describes the systems support structure as seen from the perspective of operations personnel. The first section defines the support hierarchy through which a support request may navigate. The second section defines the responsibilities for each level of support.

7.1.1 Support Hierarchy

- Network
An email or phone call must be made to the VA National Service Desk for the NSOC staff to investigate.
- Servers Hardware
After a system administrator has evaluated the problem regarding hardware or beyond his abilities to fix or repair, the Hardware Vendor – HP, needs to be contacted and their staff will require additional information to troubleshoot the problem.
- Operating systems
Each vendor (Microsoft and Red Hat) has a designated VA representative and that person should be contacted initially to help escalate the issues to the vendor's support systems.
- WebLogic
Must have a Oracle Support ID and Login to contact Oracle support. There is a POC in the VA who manages the Oracle Support Identifiers.
- SQLServer
Please follow up with the Microsoft Representative.

7.1.2 Division of Responsibilities

- Support Tier 1: National Service Desk
- Support Tier 2 : CISS/OHRS Project Staff, Primary Analysis
- Support Tier 3: SA, DBA, Developers

7.2 Support Procedures

Not applicable