Enrollment System (ES) 5.6

Production Operations Manual (POM)

May 2019

Version 5.6

Department of Veterans Affairs (VA)

Revision History

Date	Version	Description	Author
03/15/2019	5.6	5.6 updates	Liberty ITS TW
02/08/2019	5.5	5.5 updates and updated RACI	Liberty ITS TW
10/15/2018	5.4	5.4 updates	Liberty ITS TW
07/09/2018	5.3	5.3 updates	Liberty ITS TW
03/13/2018	5.2	5.2 updates	SMS/Leidos TW
02/15/2018	5.1	5.1 updates	SMS/Leidos TW
10/23/2017	5.0	5.0 updates	SMS/Leidos TW
09/19/2017	4.0	4.8 updates	SMS/Leidos TW
09/01/2017	3.0	4.7 updates	SMS/Leidos TW
05/30/2017	2.2	4.6.2 updates	SMS/Leidos TW
04/25/2017	2.1	4.6.1 updates	SMS/Leidos TW
03/16/2017	2.0	4.6 updates	SMS/Leidos TW
01/09/2017	1.1	4.5.1 updates	SMS/Leidos TW
12/15/2016	1.0	Initial publication	SMS/Leidos TW

Note: The revision history cycle begins once changes or enhancements are requested, after the POM is baselined.

Artifact Rationale

The POM provides the information needed by the production operations team to maintain and troubleshoot the product. The POM must be provided prior to release of the product.

Table of Contents

1. Introduction

The mission of the VA Office of Information and Technology (OIT), Enterprise Program Management Office (EPMO) is to provide benefits to Veterans and their families. To meet this overarching goal, OIT is charged with providing high quality, effective, and efficient IT services, and Operations and Maintenance (O&M) to persons and organizations that provide point-of-care services to our Veterans.

The VA's goals for its Veterans and families include:

- Make it easier for Veterans and their families to receive the right benefits, and meeting their expectations for quality, timeliness, and responsiveness.
- Improve the quality and accessibility of health care, benefits, and memorial services while optimizing value.
- Provide world-class health care delivery, by partnering with each Veteran to create a personalized, proactive strategy to optimize health and well-being, while providing state-of-the-art disease management.
- Ensure awareness and understanding of the personalized, proactive, and patient-driven healthcare model through education and monitoring.
- Provide convenient access to information regarding VA health benefits, medical records, health information, expert advice, and ongoing support needed to make informed health decisions and successfully implement the Veterans' personal health plans.
- Receive timely, high-quality, personalized, safe, effective, and equitable health care, not dependent upon geography, gender, age, culture, race, or sexual orientation.
- Strengthen collaborations with communities and organizations, such as the Department of Defense (DoD), Department of Health and Human Services (DHHS), academic affiliates, and other service organizations.

To assist in meeting these goals, the Enterprise Health Benefits Determination (EHBD) program will provide enterprise-wide enhancements and sustainment for the following systems/applications:

- The Enrollment System (ES) assists Veterans to enroll for VA healthcare benefits and is the core application that feeds other VA systems with Enrollment and Eligibility (E&E) data.
- Income Verification Match (IVM) assists in determining priority grouping for healthcare eligibility.
- Veterans Health Information Systems and Technology Architecture (VistA) Registration, Eligibility & Enrollment (REE) shares information with other VistA applications and enables registration and eligibility determinations and enrollment at VA Medical Centers (VAMC).
- Veterans On-Line Application (VOA) is re-purposed for the online Veterans Health Benefits Handbook (VHB). VHB provides each enrolled Veteran on-demand online access to a personalized and dynamic health benefits-related handbook.

Enrollment System Modernization (ESM) defines health benefit plans for which a client (Veteran, service member, or beneficiary) is eligible and ties them to the authority for care. Key enhancements to be completed include Pending Eligibility Determination, fixes to the Enrollment System, Date of Death (DOD), internal controls, workflow, Veterans Financial Assessment, converting of Military Service Data Sharing (MSDS) to Enterprise Military Information Service (eMIS), manage relationships, Veteran Contact Service, and support for Enrollment System Community Care (ESCC).

Veterans Health Administration (VHA) Chief Business Office (CBO) is the business owner for ES and Health Eligibility Center (HEC) is the main system user. HEC is VHA's authoritative source for enrollment and eligibility activities, which support the delivery of VA healthcare benefits.

ES is a Java application that utilizes the Java 2 Enterprise Edition (J2EE) platform architecture. It consists of two major sub-systems or modules: messaging and case management. The messaging sub-system provides a seamless bidirectional interface with external VHA and non-VHA systems for data exchange of Veterans information. The case management sub-system is an intranet Web-based application that provides authorized VHA case representatives at the HEC with a Web interface to easily track, maintain, and manage cases associated with Veteran benefits.

2. Routine Operations

This section describes procedures and tasks required for normal operations of the system.

2.1. Administrative Procedures

2.1.1. System Startup

Refer to the Administration Console for administrative procedures regarding WebLogic administration tasks. Tasks such as system startup, system shutdown, and backup and restore are managed by the Austin Information Technology Center (AITC) and handled by the AITC system administrators. Using the Administration Console, more detailed information on WebLogic administration tasks can be obtained from the official documentation at:
Oracle WebLogic Server on Oracle Fusion Middleware 12c (12.2.1.2.0)

2.1.1.1. System Startup from Emergency Shutdown

System startup is managed by the AITC and handled by the AITC system administrators.

2.1.2. System Shutdown

System shutdown is managed by the AITC and handled by the AITC system administrators.

2.1.2.1. Emergency System Shutdown

Emergency system shutdown is managed by the AITC and handled by the AITC system administrators.

2.1.3. Backup and Restore

Backup and restore operations are managed by the AITC and handled by the AITC system administrators.

2.1.3.1. Backup Procedures

Backup operations are managed by the AITC and handled by the AITC system administrators.

2.1.3.2. Restore Procedures

Restore operations are managed by the AITC and handled by the AITC system administrators.

2.1.3.3. Backup Testing

Backup testing is managed by the AITC and handled by the AITC system administrators.

2.1.3.4. Storage and Rotation

Storage and rotation operations are managed by the AITC and handled by the AITC system administrators.

2.2. Security/Identity Management

The ES application is integrated with the Web-based enterprise-level authentication services using CA SiteMinder provided by Identity and Access Management (IAM).

The Administrative Data Repository (ADR) database team is responsible for maintaining an audit trail. The team maintains an audit log at the application level. Changes to user information are tracked through ES, which automatically records additions and deletions. Currently, ES administrators generate and review the audit log for security purposes on a daily basis, and the Information Security Officer (ISO) generates and reviews the audit log on a weekly basis. ES maintains audit trails that are sufficient in assisting in reconstruction of events due to a security compromise or malfunction.

The audit trail of ES contains the following requirements:

- Identity of each person and device having access or attempting access to the system
- Date and time of the access and logoff
- Activities that modify, bypass, or negate IT security safeguards controlled by the computer system
- Security-relevant actions associated with processing
- User ID for unsuccessful logon attempts

Note: Access to online security audit logs is strictly enforced. Only the Data Base Administrator (DBA) and ISO are authorized to access the security audit logs. In addition, audit trails are reviewed following a known system violation or application software problem that has occurred. If discrepancies are identified, the information in the audit trail provides the means for a thorough investigation.

2.2.1. Identity Management

ES ensures that each user is authenticated before access is permitted. HEC users must submit a request for an ES role in order to gain access to the system; ES uses Personal Identity Verification (PIV) authentication through Single Sign-on Internal (SSOi). Users are granted a role in ES when access is approved. Accounts that are inactive for 90 days are disabled.

2.2.2. Access Control

The controls to access ES for the user and user classes are controlled through the ISO located at the HEC. In addition, the access of business roles is controlled and monitored through the HEC ISO; however, specific roles are defined within the ES application. The HEC ISO controls the population of the user groups across the domain but the AITC controls the access groups.

Note: Details are described in the AITC Directive 0712 (Parts: 16 General User Security Procedures and 20 System Administrator Security Procedures) and HEC-18.

Application users are restricted from accessing the operating system, applications, or other system resources not required in the performance of their duties. Authorized Web services staff monitors the security log regularly to detect any instances of unauthorized transaction attempts. The system will automatically end the user's session after 20 minutes of inactivity.

Listed below are the following recommended users/security keys/roles:

- Local Administrator/ISO/Report Viewer – Data Quality Manager (DQM)
- System Administrator/Information Resource Manager (IRM)/Report Viewer – Legal Administrative Specialist (LAS)
- Eligibility/Enrollment (EE) LAS/Report Manager – Everything/Report Viewer – Program Support Clerk (PSC)
- EE Supervisor/Report Manager – DQM/Report Viewer – SSN
- Director/Report Manager – PSC/Undeliverable Mail Manager
- EE Program Clerk/Report Viewer–Everything/Enrollment Group Threshold (EGT) Manager
- VistA Clerk/Report Viewer – Non-HEC/IV LAS
- Call Center Clerk/Report Viewer – HEC

Note: Federal policies require that all IT positions are evaluated and that a sensitivity level is assigned to the position description. A background investigation is required for all VHA employees filling sensitive positions. VHA personnel and non-VHA personnel, including contractors, must have

personnel security clearances commensurate with the highest level of information processed by the system.

User access is restricted to the minimum necessary to perform the job. Each ES user is assigned privileges that allows or restricts updating, deleting, and/or inserting records in the database. In addition, ES uses application-level security controls to limit access to various system functions to only authorized users.

2.3. User Notifications

The Enterprise Service Desk (ESD) will be notified of any system outages. ESD will release an Automated Notification Reporting (ANR) message informing all users of the affected system(s), status, and expected time the system will be operational (for scheduled outages).

2.3.1. User Notification Points of Contact

In the case of a system outage, system or software upgrades to include scheduled or unscheduled maintenance, or system changes, the following organizations listed in Table 1 are notified by ANR and email—at or before the time of ANR creation—approximately 5-7 days prior to deployment. There is no specific priority assigned to notifications.

Table 1: User Notification Points of Contact

Organization	Email Address
HEC	REDACTED
Change Healthcare	commandcenter@changehealthcare.com
VOA	OIT EPMO TRS EPS SoS Weblogic Support REDACTED
Veteran Information Eligibility Record Services (VRS)	REDACTED
National Health Information (NHI)	REDACTED
IVM/Enrollment Database (IVM/EDB)	REDACTED
Healthcare Claims Processing System (HCPS)	REDACTED
Veterans Health ID Card (VHIC)	REDACTED

2.4. System Monitoring, Reporting and Tools

This section describes a high-level overview of the monitoring for the ES production environment.

2.4.1. Dataflow Diagram

Figure 1 is an overview diagram of the internal and external systems and sub-systems that interface with the ES and shows the data stores that ES shares with other systems.

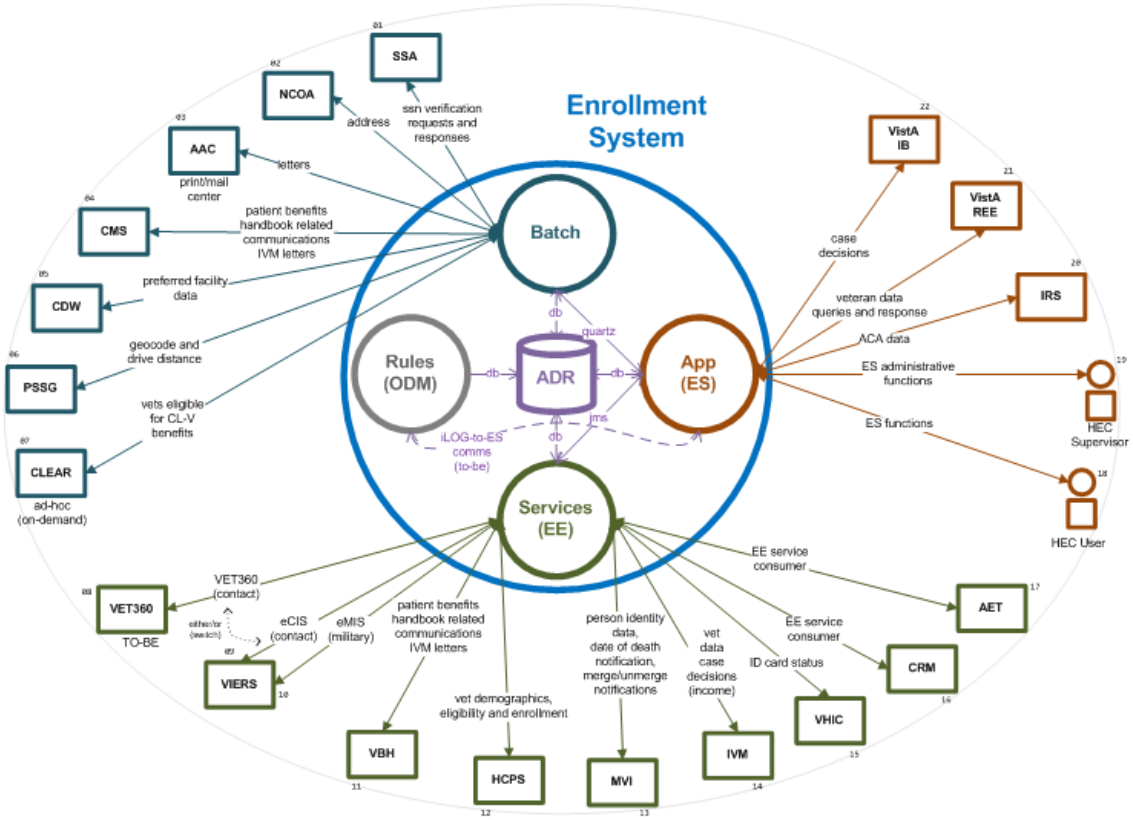

Figure 1: Dataflow Diagram

2.4.2. Availability Monitoring

The system is monitored by AITC using the tools CA Introscope and BlueStripe. The tools can be accessed via the URL: REDACTED

You need to be in the CA APM Application Environment Tool in order to access Introscope and BlueStripe.

Monitoring tool alerts describe the various system components that are being monitored for various parameters, as seen in Figure 2.

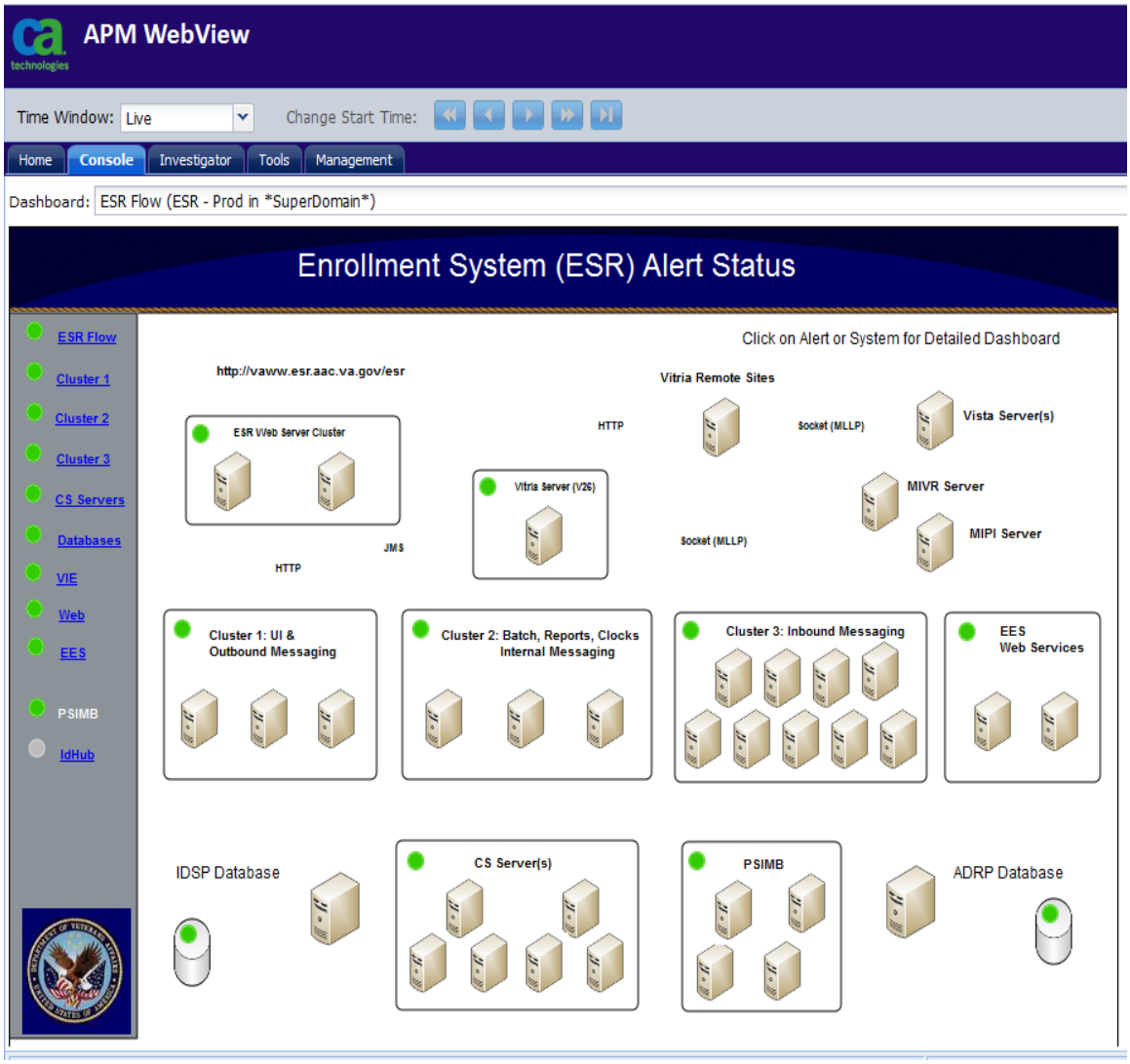

Figure 2: Introscope Alert Dashboard

2.4.3. Performance/Capacity Monitoring

There are a number of metrics captured via the Introscope Server:

- Central Processing Unit (CPU) utilization
- Memory utilization
- WebLogic Java Messaging Service (JMS) queues current and pending count
- WebLogic JMS queues response time
- CPU per Java process
- Garbage collection pattern

- Managed server status
- Web module average response time
- Backend database average response time
- Web service response time
- Connectivity with other systems such as VistA Interface Engine (VIE) and Person Service Identity Management (PSIM)

These metrics can be browsed for either real time data, or for a selected period of time. A sample graph is shown in Figure 3.

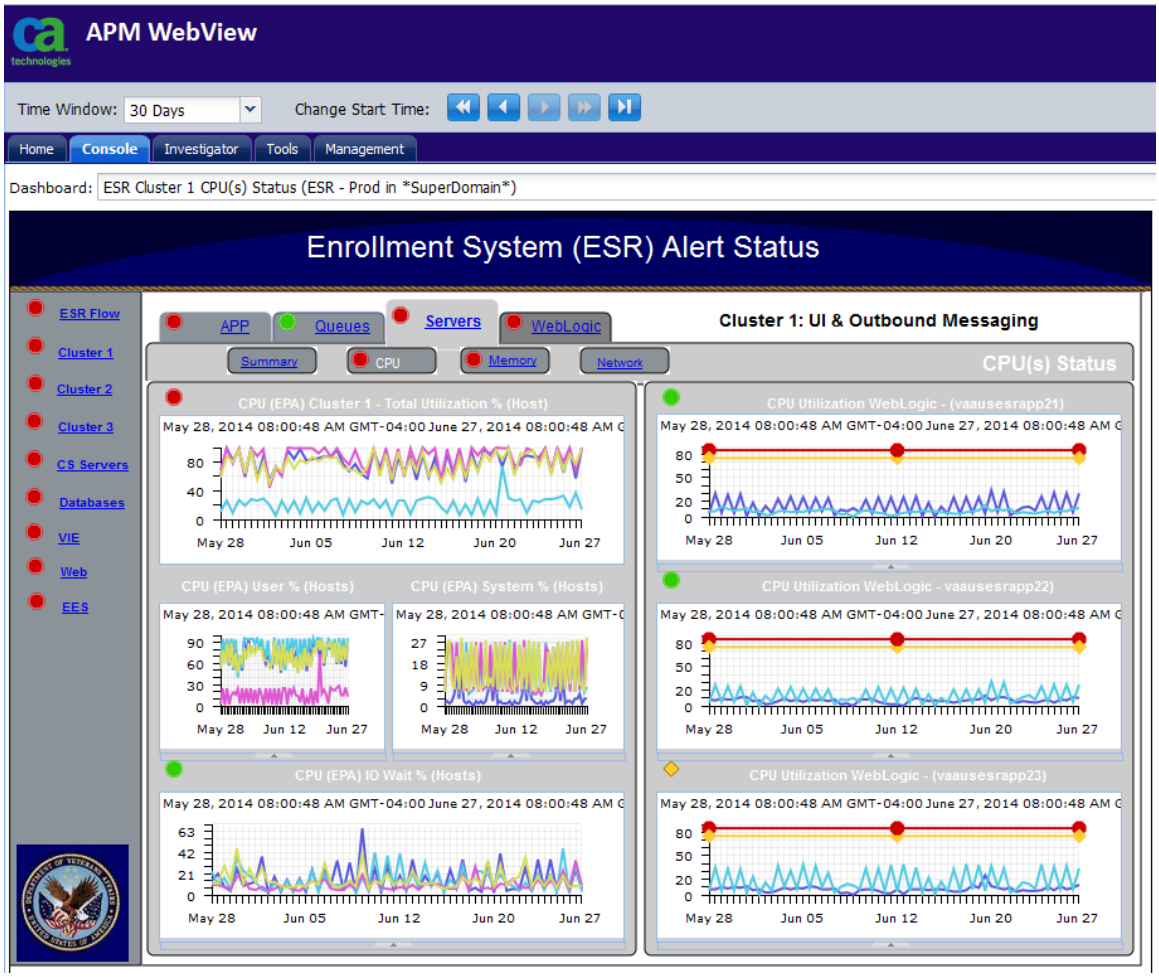

Figure 3: Sample ES Performance Monitoring Graph

2.4.4. Critical Metrics

The critical metrics captured for ES are covered in Section 2.4.3, Performance/Capacity Monitoring.

2.5. Routine Updates, Extracts and Purges

There are no additional maintenance activities required for ES.

2.6. Scheduled Maintenance

The ES has scheduled maintenance on the third Saturday of each month. Prior to each scheduled maintenance window, the ESD is notified and an ANR released to notify all users.

2.7. Capacity Planning

Capacity planning for each release starts in the requirements phase. The steps are as follows:

- Analyze the requirements and identify changes in the following areas:
  a. Increase in messaging volume and pattern
  b. Increase in Web service request volume and pattern
  c. Volume of records processed by batch processes
  d. Data storage increase
  e. File storage increase
  f. Performance requirements
- Assess current capacity usage against the new needs
- Plan and Initiate Service requests for additional infrastructure if needed

2.7.1. Initial Capacity Plan

Figure 4 shows the current total top 10 activities (Event) based on over four million activities by frequency. These activities impact the ADR and VistA databases, however with non-CPU/WAN/LAN intensity.

Event	Frequency	Database Impact	Database Growth / transaction	Average Message Size	Protocol Used	CPU Intensive	WAN Intensive	LAN Intensive
ORUZ11	1.2m/day	ADR VistA	>0<1.49MB	5 KB	HL7	N	N	N
1305	1.1m/day	ADR	>0<1.49MB	4 KB	SOAP	N	N	N
1309	700k/day	ADR	>0<1.49MB	3 KB	SOAP	N	N	N
ORUZ07	400k/day	ADR VistA	>0<1.49MB	5 KB	HL7	N	N	N
ORUZ05	270k/day	ADR VistA	>0<1.49MB	4 KB	HL7	N	N	N
ORYZ10	230k/day	ADR VistA	>0<1.49MB	1 KB	HL7	N	N	N
ORFZ10	210k/day	ADR VistA	>0<1.49MB	4 KB	HL7	N	N	N
ORUZ10	60k/day	ADR VistA	>0<1.49MB	4 KB	HL7	N	N	N
ORYZ11	11k/day	ADR VistA	>0<1.49MB	1 KB	HL7	N	N	N
ORFZ11	9k/day	ADR VistA	>0<1.49MB	4 KB	HL7	N	N	N

Figure 4: Top 10 Business Events

3. Exception Handling

This section provides a high-level view of system errors that may be encountered during operation.

3.1. Routine Errors

Like most systems, ES may generate a small set of errors that may be considered 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 subsections 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 large numbers of individual errors 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.

3.1.1. Security Errors

Security errors encountered by users and/or operators will involve login and privilege issues. These will typically involve a user not having the appropriate access levels granted. These can be corrected by contacting the appropriate security administrator or the VA help desk.

3.1.2. Time-outs

Session time-outs may occur to end a user's session if it is left unattended for an extended period of time. The user will need to establish a new session by logging in and resuming the work in progress.

3.1.3. Concurrency

Concurrency errors may be encountered by users attempting to update a case or other business records at the same time as another user. This is an extremely rare occurrence due to the way cases are assigned to users, and to the fact that the user base is relatively small. If this does occur, the first user will take precedence and the second user will be notified that any changes made during the session will not be written to the database. This type of optimistic locking assumes low likelihood of occurrence and will prevent inadvertent corruption of data.

3.2. Significant Errors

Significant errors are errors or conditions that affect the system stability, availability, performance, or make the system unavailable. The following subsections can help administrators, operators, and other support personnel resolve significant errors, conditions, or other issues.

3.2.1. Application Error Logs

This section provides information regarding the logging capabilities of the system.

The ES application is hosted by a WebLogic Domain of clustered servers. The domain consists of one Admin server instance, ESRAdminServer, and three managed servers (MS1, MS2 and MS3).

Each subsystem within WebLogic Server generates server log messages to communicate its status. To keep a record of the messages that the subsystems generate, WebLogic Server writes the messages to log files. The server log records information about events, such as the startup and shutdown of servers, the deployment of new applications, and the failure of one or more subsystems. The messages include information about the time and date of the event, as well as the ID of the user who initiated the event.

In addition to writing messages to a log file, each server instance prints a subset of its messages to the standard output log. By default, a server instance prints only messages of a WARNING severity level or higher to the standard output log.

The messages for all WebLogic Server subsystems contain a consistent set of fields (attributes) as described in Table 2.

Table 2: Log Message Attributes

Attribute	Description
Timestamp	Time and date when the message originated, in a format that is specific to the locale. The Java Virtual Machine (JVM) that runs each WebLogic Server instance refers to the host computer's operating system for information about the local time zone and format.
Severity	Indicates the degree of impact or seriousness of the event reported by the message
Subsystem	Indicates the subsystem of WebLogic Server that was the source of the message. For example, Enterprise Java Bean (EJB) container or Java Messaging Service (JMS)
Server Name Machine Name Thread ID	Identify the origins of the message: Server Name is the name of the WebLogic Server instance on which the message was generated. Machine Name is the Domain Name Server (DNS) name of the computer that hosts the server instance. Thread ID is the ID that the JVM assigns to the thread in which the message originated. Log messages that are generated within a client JVM client do not include these fields. For example, if an application runs in a client JVM and it uses the WebLogic logging services, the messages that it generates and sends to the WebLogic Server log files will not include these fields.
User	The user ID under which the associated event was executed. To execute some pieces of internal code, WebLogic Server authenticates the ID of the user who initiates the execution and then runs the code under a special Kernel Identity user ID. J2EE modules such as EJBs that are deployed onto a server instance report the user ID that the module passes to the server. Log messages generated within a client JVM client do not include this field.
Transaction ID	Present only for messages logged within the context of a transaction.
Message ID	A unique six-digit identifier All message IDs that WebLogic Server system messages generate start with BEA- and fall within a numerical range of 0-499999.
Message Text	A description of the event or condition

The **severity** attribute of a WebLogic Server log message indicates the potential impact of the event or condition that the message reports.

Table 3 lists the severity levels of log messages from WebLogic Server subsystems, the lowest to highest impact level. WebLogic Server subsystems can generate many lower severity messages and a few high severity messages (e.g., under normal circumstances, they can generate many `INFO` messages and no `EMERGENCY` messages).

Table 3: Message Severity

Severity	Meaning
INFO	Used for reporting normal operations.
WARNING	A suspicious operation or configuration has occurred but it might not affect normal operation.
ERROR	A user error has occurred. The system or application can handle the error with no interruption and limited degradation of service.
NOTICE	An INFO or WARNING-level message that is particularly important for monitoring the server. **Note:** Only WebLogic Server and its subsystems generate messages of this severity.
CRITICAL	A system or service error has occurred. The system can recover but there might be a momentary loss or permanent degradation of service. **Note:** Only WebLogic Server and its subsystems generate messages of this severity.
ALERT	A particular service is in an unusable state while other parts of the system continue to function. Automatic recovery is not possible; the immediate attention of the administrator is needed to resolve the problem. **Note:** Only WebLogic Server and its subsystems generate messages of this severity.
EMERGENCY	The server is in an unusable state. This severity indicates a severe system failure or panic. **Note:** Only WebLogic Server and its subsystems generate messages of this severity.

When a WebLogic Server instance writes a message to the log file, the first line of each message begins with `####` followed by the message attributes. Each attribute is contained between angle brackets.

The following is an example of a message in a log file:

```
####<Sep 12, 2017 12:00:34 PM CDT> <Info> <Diagnostics> <REDACTED <MS1>
<[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default (self-
tuning)'> <<WLS Kernel>> <> <> <1505235634542> <BEA-320145> <Size based
data retirement operation completed on archive EventsDataArchive.
Retired 0 records in 1 ms.>
```

In this example, the message attributes are: Timestamp, Severity, Subsystem, Machine Name, Server Name, Thread ID, User ID, Transaction ID, Message ID, and Message Text.

- If a message is not logged within the context of a transaction, the angle brackets for Transaction ID are present even though no Transaction ID is present.
- If the message includes a stack trace, the stack trace follows the list of message attributes.

When a WebLogic server instance writes a message to the standard output log, the output does not include the `####` prefix and does not include the Server Name, Machine Name, Thread ID, and User ID fields.

The following is an example of how the message from the previous section would be printed to the standard output log:

```
<Sep 12, 2017 11:05:59 AM CDT> <Info> <Security> <BEA-090905>
<Disabling CryptoJ JCE Provider self-integrity check for better startup
performance. To enable this check, specify -
Dweblogic.security.allowCryptoJDefaultJCEVerification=true>
```

In this example, the message attributes are: Timestamp, Severity, Subsystem, Message ID, and Message Text.

Each WebLogic Server instance writes all messages from its subsystems and applications to a log file that is located on the local host computer.

In addition to writing messages to its local log file, each server instance forwards a subset of its messages to a domain-wide log file. By default, servers forward only messages of severity level ERROR or higher.

The ES application uses Log4j logging framework, which makes it possible to enable logging at runtime without modifying the application.

Log files can be accessed using a Web log portal called REDACTED.

The log files (server and domain) and standard output log files are located on the application servers and can also be accessed using SSH to servers. The servers have the .log and .out files located below the server root directory in logs directory.

```
./servers/<serverName>/logs/<serverName>.log
./servers/<serverName>/logs/<serverName>.out
```

The Log4j log files are created in the $DOMAIN_HOME directory

```
./esr_<serverName>.log
```

3.2.2. Application Error Codes and Descriptions

All application errors are logged. The ES does not generate error codes, but produces and logs Java style exceptions.

3.2.3. Infrastructure Errors

Common errors displayed by the ES due to interactions with external systems are described in the Dependent Systems section.

3.2.3.1. Database

All database errors are logged in the application error log.

3.2.3.2. Web Server

All Web server errors are logged in the application error log. In addition to server logs, Hypertext Transfer (or Transport) Protocol (HTTP) logging is enabled on each server and the server saves HTTP requests in a separate log file, named *access.log* in

```
./servers/<serverName>/logs/access.log
```

3.2.3.3. Application Server

All application server errors are logged in the application error log.

3.2.3.4. Network

N/A
Network errors can arise due to many factors, and are often beyond the extent of the ES system. For this reason, network errors are not applicable.

3.2.3.5. Authentication & Authorization

The application error log includes authentication and authorization errors caused by interactions with external systems.

3.2.3.6. Logical and Physical Descriptions

From an application perspective, the ES is designed following layering and Service Oriented architectural framework. Logically, the system is segmented under two major components: the enterprise framework and the application component. The enterprise framework consists of low-level system plumbing and management critical to any large mission critical system, including transaction management, security, data access layer and many more. The application component resides on top of the enterprise framework and is responsible for the business processes.

The ES application (formerly ESR) is comprised of four major modules: Framework, Common, User Interface (UI), and Messaging. Each of these modules is an independent set of services that are consumed by other external or internal clients.

- The framework module represents the system plumbing and integration points with other third-party libraries.
- The common module represents the application layer component consumed by the messaging, workflow, communication, and the UI modules.
- The messaging module is the integration point between ES and other external applications. This module allows for asynchronous and synchronous communication protocols.
- The UI module is the presentation layer of ES. The end users access this module through a Web interface, hosted on the VHA network.

Figure 5 is a diagram of the ES Application Architecture Overview of the ES application.

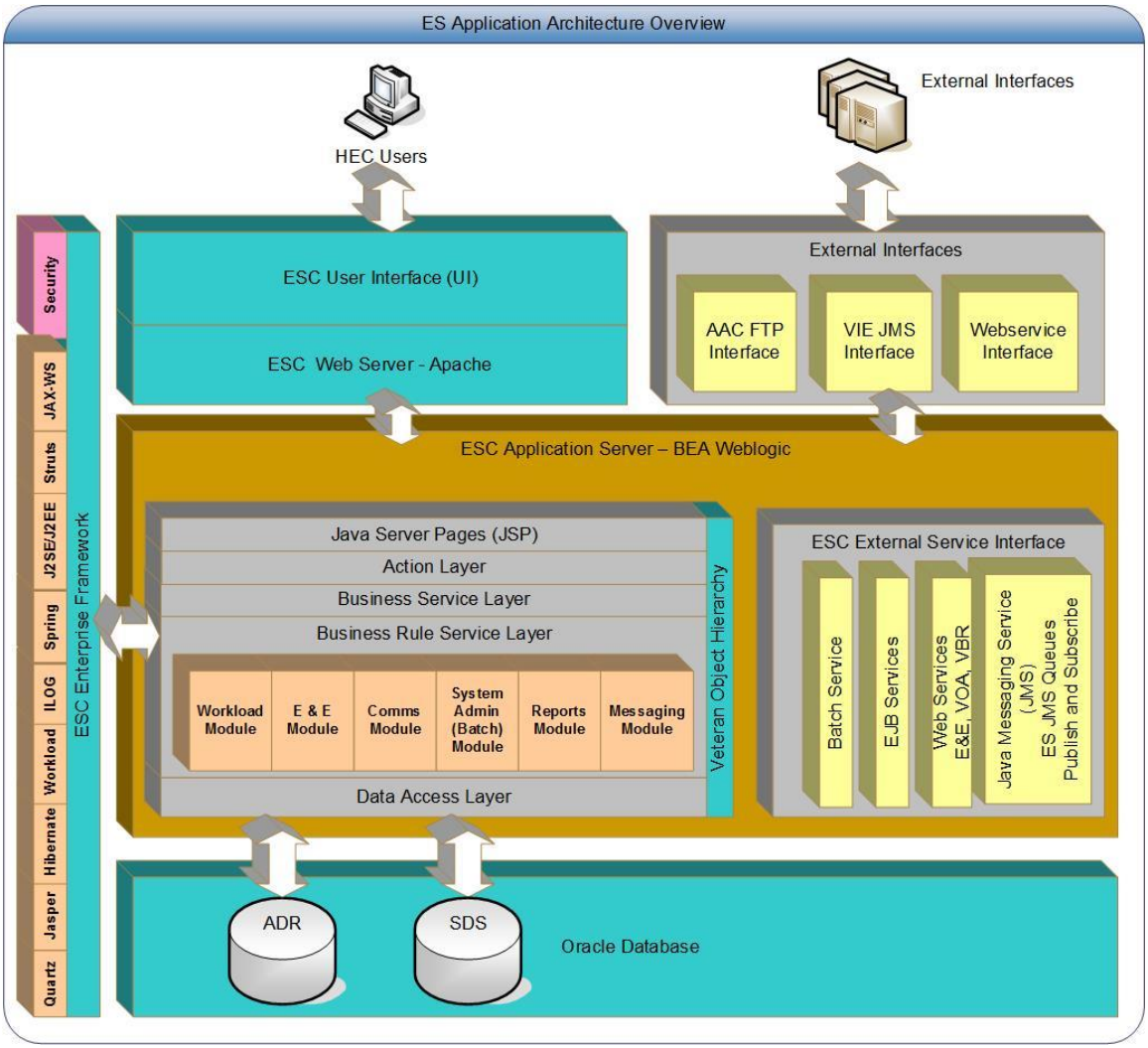

Figure 5: ES Application Architecture Overview

The ES Physical Architecture outlines the hardware components that represent the environments mentioned in Figure 6. The Web-tier is represented by a series of Web servers, the business-tier is represented by a series of application servers in clustered environment, and the enterprise information data tier is represented by pure database servers. The following sections define the ES platform with hardware and software specifications:

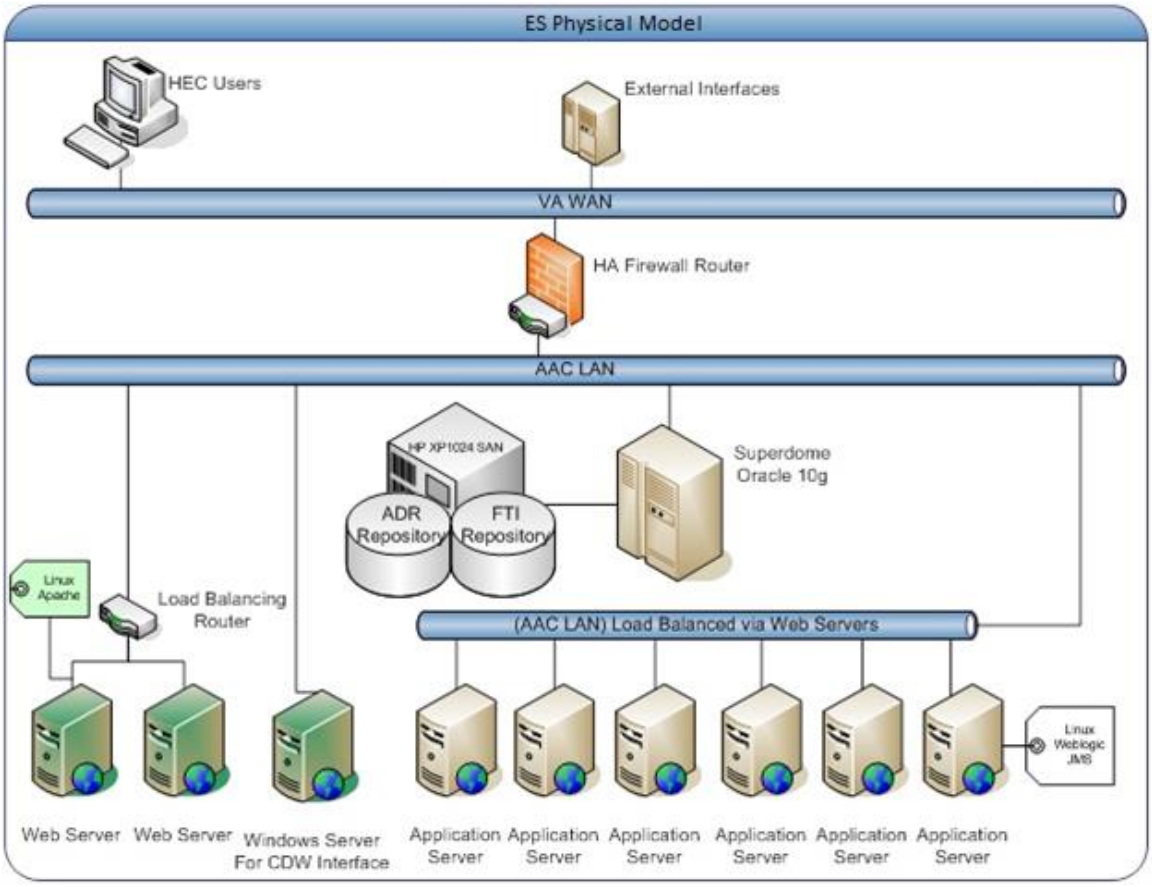

Figure 6: ES Physical Model

The ES Physical view in Figure 7 represents the deployed environment and the relationship between the different software packages and hardware components residing on the ES platform.

REDACTED

Figure 7: ES Production Configuration

AITC maintains the hardware specifications in a configuration management database.

3.3. Dependent System(s)

Table 4 lists the systems used by ES.

Table 4: ES Dependent Systems

Internal or External	Name	Description	Interface Name	Interface System
External	Social Security Administration (SSA)	To verify Social Security numbers (SSN)	SSN Verification	SSA
Internal	AITC Mail Center	To print and mail letters to Veterans	Letters Interface	AITC mainframe
Internal	VistA REE	To receive and send Veteran data	Messaging Interface	VistA Health Level 7 (HL7)
Internal	VistA Integrated Billing (IB)	To share IVM conversion decisions	Messaging interface	VistA IB
Internal	Master Veteran Index (MVI)	To retrieve primary view traits, update person traits, receive Date of Death Notification, receive merge/unmerge notifications on person Integration Control Number (ICN)	MVI interface	MVI Person Service Identity Management (PSIM)
Internal	Veteran Information/Eligibility Record Services (VIERS)	Enrollment Data to support Affordable Care Act (ACA) and eMIS queries from the Content Management System (CMS)	ACA interface	VIERS
Internal	VA/DoD Identity Repository (VADIR)	To retrieve military service data	Enterprise Military Information Service (eMIS)	VADIR/ Beneficiary Identification Records Locator System (BIRLS)
Internal	Corporate Data Warehouse (CDW)	To retrieve primary care provider data	Preferred Facility	CDW
External	CMS	To print and mail handbooks and inserts	Handbook	NPC
Internal	IVM	To share person data and receive case decisions	IVM bidirectional	IVM

Internal or External	Name	Description	Interface Name	Interface System
		(conversions/reversals) and predetermine the enrollment		
Internal	Veterans Benefits Handbook	To allow Veterans to access on-demand personalized and dynamic health benefits-related handbook	Handbook Portal	VOA
External	National Change of Address (NCOA)	To receive address corrections	Address Verification	NCOA
Internal	Master Veteran Record (MVR)	Sending of solicited eligibility/enrollment information and the receiving of unsolicited eligibility/enrollment information	MVR	Veterans Benefit Administration (VBA)
Internal	VistA	Sending of solicited eligibility/enrollment information and the receiving of unsolicited eligibility/enrollment information	VistA	VistA REE
Internal	VHIC	Query Veteran's identity card details and status	VHIC interface	VHIC
External	Internal Revenue Service (IRS)	Service provider for the 1095B coverage period transactions	IRS	IRS
External	Third Party Administrators (TPA)	Sending Community Care (CC) eligibility and demographics data	TPA	Secure File Transfer Protocol (SFTP)
External	Community Care Network (CCN) contractors	Sending CC eligibility and demographics data	CCN	Data Access Services (DAS)
Internal	VET360	Authoritative contact information service for validating delivery point on addresses	VET360	VET360

3.4. Troubleshooting

This section provides information to assist with resolving error conditions that may be encountered with the ES.

Scenario 1: Missing Inbound Message

Troubleshooting Steps

1. Which site sent the message?

   This can be found in the BHS segment. In the below example, the Z07 came from VA Medical Center (VAMC) 552.

   BHS^~|\&^VAMC
   552^552^ESR^200ESR^20040810^^~T~ORU|Z07~2.3.1~AL~AL^^54364365^

2. What are the Batch Control Number and Message Control Number?

   In the below example, 54364365 is the batch control number and 88865050-1 is the message control number.

   BHS^~|\&^VAMC
   552^552^ESR^200ESR^20040810^^~T~ORU|Z07~2.3.1~AL~AL^^54364365^

   MSH^~|\&^VAMC 552^552^ESR^200ESR^20030904121212-
   0500^^ORU~Z07^88865050-1^T^2.1^^^AL^AL^USA

3. What Person is contained in the HL7 message?

   The Data File Number (DFN) is in the PI section of the PID segment. In this example, 55202 is the DFN.

   PID^1^1000913833V082573^1000913833V082573~~~USVHA&&0363~NI~VA
   FACILITY ID&200M&L|55202~~~

   USVHA&&0363~PI~VA FACILITY
   ID&500&L|000004834~~~USSSA&&0363~SS~VA FACILITY
   ID&500&L|666123456~~~USSSA&&0363~SS~VA FA

   CILITY ID&500&L~~20060127|000123456~~~USSSA&&0363~SS~VA FACILITY
   ID&500&L~~20060127^^ESRPATIENT~FNAME~X~~~^^19270101^M^^^557
   OREGONS~""~LITTLE FALLS~NY~13333-1633~USA~VACAE~STE
   322~~~~20020125&20060125|3400 EDS DRIVE~""~HERNDON~VA~20171-
   1633~USA~P~STE 322~~~~20020125&20060125^^

   (999)123-0001~PRN~PH|(999)123-0002~WPN~PH|(999)123-0003~ORN~CP|(999)123-
   0004~BPN~BP|~NET~INTERNET~EMAIL@FOO.COM^(999)123-0005X3464

   ^^^^^1346

4. When was the message sent?

   The message below was sent on 8/10/2004

   BHS^~|\&^VAMC
   552^552^ESR^200ESR^20040810^^~T~ORU|Z07~2.3.1~AL~AL^^54364365^

5. Query the database for the message.

If the message is not found in the database then either ES has not received it, or it is still in the inbound JMS queue waiting to be processed.

Find a Message by Message Control Id (replace number)

Select message_control_number, record_created_by, to_char(record_created_date, 'mm/dd/yyyy hh:mi:ss') from hl7_transaction_log where message_control_number='88865050-1’

6. Look at the backlog of messages on JMS queue (using Introscope).

   Note: A high volume of messages in MessagesCurrentCount for a particular JMS queue would indicate that there are messages that ES has not yet processed.

7. Check with VIE, as to the status of the message

   VIE will typically need the Batch Control ID to track it down in their JMS queues.

Scenario 2: Missing Outbound Message

Troubleshooting Steps

1. First look in the HL7_TRANSACTION_LOG table for the Message Control ID.

   Select message_control_number, record_created_by, to_char(record_created_date, 'mm/dd/yyyy hh:mi:ss') from HL7_transaction_log where message_control_number='88865050-1’

2. If it is not found in HL7_TRANSACTION_LOG, then check whether ES triggered this outbound message at all?

   Look in triggerEvent.log in XpoLog

   Note: Search for personId=xxx

3. Is there a Consistency Check failure that occurred in Cluster1?

   The following would be found in the esr.log for the outbound managed server:

   [ERROR] 21 Aug 03:45:25.567 PM ExecuteThread: '8' for queue: 'OutboundMessageThreadPool' [REDACTEDmessaging.util.MessagingWorkloadCaseHelper]

   Create ConsistencyCheck WorkloadCase for group [Enrollment Eligibility] and target Person [133156322] for target Message [ORUZ05-S]

4. Is there a Workload Case created?

   Replace with personId and *n* in the following.

   Select * from wkf_Case where person_ID=2 and rownum<20 order by record_created_date desc

5. Look in esr.log in Cluster1.
6. If everything looks okay in ES, contact the VIE team, giving them the Batch Control ID or Message Control ID.

Scenario 3: Batch Process Taking Too Long

Troubleshooting Steps

1. Confirm if the batch process is still running. This may not always be straightforward.
    - Look for the batch process' execution in the esr.log file.

      [INFO] 22 Aug 03:10:00.043 AM ExecuteThread: '13' for queue: 'InternalEventThreadPool' [REDACTEDbatchprocess.BatchProcessServiceImpl] Executing job/process [scheduledJob.dataSynchronizationHECLegacyProducer] for executionContext/user [AUTO_PER_SCHEDULE]
    - Find the thread ID running the batch process.
    - Look for subsequent log statements with the thread ID.

      [INFO] 22 Aug 03:10:01.106 AM ExecuteThread: '13' for queue: 'InternalEventThreadPool' [REDACTEDcommon.batchprocess.datasync.HECLegacyDataSynchronizationProducer Process] AbstractDataQueryIncrementalProcess acquired 65 data records
    - Do a few refreshes for the view on the Batch Processes -> Active tab. If the number of records does not change after several refreshes, then check the history of the job on the management tab. An entry with a status of NOT_EXECUTED_SINCE_INFLIGHT_PROCESS can indicate that the server restarted, and the batch job is therefore stalled.
2. If the batch process is running, look at database statistics from Prod Database Service (DBS) and/or Introscope.
3. If the batch process is not running, mark as ERROR from the user interface to clean up the view.
4. If the batch job is scheduled to execute again within 12 hours, then wait for the job to start automatically at the next scheduled start time. Otherwise, restart the job by clicking the execute hyperlink for the batch job listed on the Batch Processes tab.

Scenario 4: NumberOfErrorRecords

For a batch process, what is the reason for the numberOfErrorRecords=n, where n is not 0?

Troubleshooting Steps

1. Find the batch process' execution in esr.log.
2. Determine the thread ID.
3. Look for any exceptions that follow for that thread ID. Threads get reused once they are complete, so the thread may be used by another process later on.
4. Analyze the exceptions found, and work with Level 3 support to resolve them.

   Note: Some batch jobs write exceptions to an .exception file. The ones that do this are: IVM Producer and Austin Automation Center (AAC) Letter Export.

Scenario 5: eMIS Query Status in "Queried – Pending Response"

This scenario assumes that a Veteran record was already identified.

Troubleshooting Steps

1. Contact the "OIT EPMO TRS EPS SoS Weblogic Support" mail group in Outlook REDACTED asking them to check the status of the ES eMIS Web service.

2. Contact Tier 3 support.

Scenario 6: Users Getting No Response

Users of the ES Eligibility & Enrollment Web Service say they are not getting a response.

Troubleshooting Steps

1. Contact the "OIT EPMO TRS EPS SoS Weblogic Support" mail group in Outlook REDACTED), asking them to check the status of the ES Eligibility and Enrollment Service (EES) Web service.
2. Contact Tier 3 support.

Scenario 7: Outbound Messages Missing Troubleshooting Steps

Troubleshooting Steps

1. Contact the "OIT EPMO TRS EPS SoS Weblogic" mail group in Outlook (REDACTED asking them to check the person ID for the missing message in cluster 1 logs. If the person ID is not found, request them to check status of the messaging event queue to see if there are any pending messages in the queue.
2. Contact Tier 3 support.

Scenario 8: PSIM Web Service Interface Failing Axis Fault Error

Troubleshooting Steps

1. If you see error message like "Caused by: javax.net.ssl.SSLHandshakeException: Received fatal alert: certificate_expired".
2. Contact the "OIT EPMO TRS EPS SoS Weblogic Support" mail group in Outlook REDACTED asking them to check the logs for any certificate errors or Veterans Affairs Authentication Federation Infrastructure (VAAFI) connection errors. If there are certificate or VAAFI connectivity errors, contact the VAAFI support team (REDACTED

Scenario 9: Health Benefit Plans (HBP) Data in ES Not Being Transmitted to Sites

Troubleshooting Steps

1. Verify a Z11 was transmitted from ES to the sites; Verify the Z11 contains the ZHP segment
2. Log in to ES, then navigate to Admin -> System Parameters. Verify the system parameter named HBP Data sharing indicator is set to "Y" to enable the ZHP segment to be included in the Z11 messages to the sites.
3. Contact Tier 3 support.

Scenario 10: Enrollment Records in VistA CL = Yes Patient Not Eligible

Troubleshooting Steps

1. Verify a Z11 was transmitted from ES to the sites; Verify the Z11 contains the ZHP segment. Verify a Z11 was transmitted from ES to the sites; Verify the Z11 does not contain Camp Lejeune data on the ZEL segment.
2. Log in to ES, and then navigate to Admin -> System Parameters. Verify the system parameter named CL_VISTA_FULL_ROLLOUT is set to "ALL" or has the site in the delimited field to enable the Camp Lejeune information to be included in the Z11 messages to the sites.
3. Contact Tier 3 support.

   Note: The system parameter CL_VISTA_FULL_ROLLOUT needs to be set to "all". This is done by the HEC System Administrator when the CL-V VistA host file DG*5.3*909 is deployed to production. This system parameter should never be inactivated.

3.5. System Recovery

The process and procedures necessary for system recovery are managed by the AITC and handled by the AITC system administrators.

3.5.1. Restart after Non-Scheduled System Interruption

The process and procedures necessary to restart after a non-scheduled system interruption are managed by the AITC and handled by the AITC system administrators.

3.5.2. Restart after Database Restore

The process and procedures necessary to restart after a database restore are managed by the AITC and handled by the AITC system administrators.

3.5.3. Back-out Procedures

For back-out procedures, refer to the *ES 5.6 Deployment, Installation, Back-out, and Rollback Guide*.

3.5.4. Rollback Procedures

For rollback procedures, refer to the *ES 5.6 Deployment, Installation, Back-out, and Rollback Guide*

4. Operations and Maintenance Responsibilities

The role identification list and subsequent Responsible Accountable Consulted Informed (RACI) matrix are customized according to the requirements of each system.

Table 5: Role Identification

Name	Role	Org	Contact Info
REDACTED	Program Manager	AITC	REDACTED REDACTED
Enterprise Service Desk Dev/Ops (PD/ESE)	Enterprise Service Desk Tier 1	ITOPS	REDACTED
VA IT SDE EO EIS VHA Linux System Admins Tier 2	System Admin (Unix)	AITC	REDACTED
REDACTED	Linux Admin	AITC	REDACTED REDACTED
REDACTED	Application Manager	AITC	REDACTED REDACTED
REDACTED	Application Manager	AITC	REDACTED REDACTED
REDACTED	Sustainment Manager	AITC	REDACTED REDACTED
REDACTED	Database Administrator	AITC	REDACTED REDACTED
REDACTED	WebLogic Administrator	AITC	REDACTED REDACTED REDACTED REDACTED
REDACTED	Monitoring	AITC	REDACTED REDACTED
REDACTED	System Admin (Windows)	AITC	REDACTED REDACTED
REDACTED	Sustainment Manager	AITC	REDACTED REDACTED
REDACTED	Build Manager	AITC	REDACTED REDACTED
REDACTED	Build Manager	AITC	REDACTED

Name	Role	Org	Contact Info
			REDACTED
REDACTED	Solaris (IVM)	AITC	REDACTED REDACTED
REDACTED	Linux (IVM)	AITC	REDACTED REDACTED
REDACTED	Database Administrator (IVM)	AITC	REDACTED REDACTED
REDACTED	Messaging (IVM)	AITC	REDACTED REDACTED
Health Product Support Tier 2	Application Support	EPMO	REDACTED REDACTED
REDACTED	Program Manager EHBD	EPMO	REDACTED REDACTED
REDACTED	Project Manager ES	EPMO	REDACTED REDACTED
REDACTED	Project Manager ES	EPMO	REDACTED REDACTED
REDACTED	Technical Lead EHBD	EPMO	REDACTED REDACTED

REDACTED

5. Approval Signatures

Signed: _____

REDACTED

Signed: _____

REDACTED

Signed: _____

REDACTED

Signed: _____

REDACTED