Production Operations Manual

Genomic Information System for Integrated Science 2

(Genisis2) Technical Services

Release 3



June 2017

Document Version 3.0

Department of Veterans Affairs

Document Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| 02/10/2017 | 1.0 | Release 1 | Booz Allen Hamilton |
| 05/12/2017 | 2.0 | Release 2 | Booz Allen Hamilton |
| 06/16/2017 | 3.0 | Release 3 | Booz Allen Hamilton |

Note: The revision history cycle begins once changes or enhancements are requested after the Production Operations Manual has been baselined.

Artifact Rationale

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

Table of Contents

[1. Introduction 1](#_Toc484361842)

[2. Routine Operations 1](#_Toc484361843)

[2.1. Administrative Procedures 1](#_Toc484361844)

[2.1.1. System Startup 1](#_Toc484361845)

[2.1.1.1. System Startup from Emergency Shutdown 1](#_Toc484361846)

[2.1.2. System Shutdown 2](#_Toc484361847)

[2.1.2.1. Emergency System Shutdown 2](#_Toc484361848)

[2.1.3. Back-up & Restore 2](#_Toc484361849)

[2.1.3.1. Back-up Procedures 3](#_Toc484361850)

[2.1.3.2. Restore Procedures 3](#_Toc484361851)

[2.1.3.3. Back-up Testing 4](#_Toc484361852)

[2.1.3.4. Storage and Rotation 4](#_Toc484361853)

[2.2. Security / Identity Management 4](#_Toc484361854)

[2.2.1. Identity Management 5](#_Toc484361855)

[2.2.2. Access Control 5](#_Toc484361856)

[2.3. User Notifications 6](#_Toc484361857)

[2.3.1. User Notification Points of Contact 6](#_Toc484361858)

[2.4. System Monitoring, Reporting, and Tools 6](#_Toc484361859)

[2.4.1. Dataflow Diagram 6](#_Toc484361860)

[2.4.2. Availability Monitoring 7](#_Toc484361861)

[2.4.3. Critical Metrics 7](#_Toc484361862)

[2.5. Routine Updates, Extracts and Purges 7](#_Toc484361863)

[2.6. Scheduled Maintenance 7](#_Toc484361864)

[2.7. Capacity Planning 7](#_Toc484361865)

[2.7.1. Initial Capacity Plan 7](#_Toc484361866)

[3. Exception Handling 7](#_Toc484361867)

[3.1. Routine Errors 8](#_Toc484361868)

[3.1.1. Security Errors 8](#_Toc484361869)

[3.1.2. Time-out Errors 8](#_Toc484361870)

[3.1.3. Concurrency 8](#_Toc484361871)

[3.2. Significant Errors 8](#_Toc484361872)

[3.2.1. Application Error Logs 8](#_Toc484361873)

[3.2.2. Application Error Codes and Descriptions 8](#_Toc484361874)

[3.2.3. Infrastructure Errors 8](#_Toc484361875)

[3.2.3.1. Database 8](#_Toc484361876)

[3.2.3.2. Web Server 9](#_Toc484361877)

[3.2.3.3. Application Server 9](#_Toc484361878)

[3.2.3.4. Network 9](#_Toc484361879)

[3.2.3.6. Logical and Physical Descriptions 9](#_Toc484361880)

[3.3. Dependent System(s) 10](#_Toc484361881)

[3.4. Troubleshooting 10](#_Toc484361882)

[3.5. System Recovery 10](#_Toc484361883)

[3.5.1. Restart after Non-Scheduled System Interruption 10](#_Toc484361884)

[3.5.2. Restart after Database Restore 10](#_Toc484361885)

[3.5.3. Back-out Procedures 10](#_Toc484361886)

[3.5.4. Rollback Procedures 10](#_Toc484361887)

[4. Operations and Maintenance Responsibilities 11](#_Toc484361888)

[5. Approval Signatures 12](#_Toc484361889)

# Introduction

The Production Operations Manual describes how to maintain the components of the Genomic Information System for Integrated Science 2 (Genisis2),as well as how to troubleshoot problems that might occur with this application in production. The intended audience for this document are the Information Technology (IT) teams responsible for hosting and maintaining the application after production release. This document is normally finalized just prior to production release and includes many updated elements specific to the hosting environment.

# Routine Operations

Table 1 lists the routine operations for Genisis2.

Table 1: Routine Operations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Routine Operation** | **Periodicity** | **Role performing the Function** | **Additional External Systems, if Needed** | **Additional Description** |
| System Login Availability from the VA Network | Daily | Genisis2 System Administrator (Super User) | None | Verifies that the system is up and running. |
| Systems Monitoring and Alerting, Escalation | Real time 24/7 | Genisis2 System Administrator (Super User) | VA Systems Monitoring and Alerting Facilities | Monitors each of the Web, Application and Data Servers status. They need to be up and running |

## Administrative Procedures

### System Startup

Table 2 provides the system startup procedures for the Genesis2 servers.

Table 2: System Startup

| **Component** | **Procedure** | **Additional Comments** |
| --- | --- | --- |
| Apache Server | sudo service httpd start | TBD |
| Genisis2 Application Wildfly Server | nohup ./standalone.sh & | TBD |

#### System Startup from Emergency Shutdown

In the event of an emergency shutdown, Table 3 lists the system startup procedures for the Genesis2 servers.

Table 3: System Startup from Emergency Shutdown

|  |  |  |
| --- | --- | --- |
| **Component** | **Procedure** | **Additional Comments** |
| Apache Server | sudo service httpd start | TBD |
| Genisis2 Application Wildfly Server | cd /opt/wildfly  nohup ./standalone.sh & | TBD |

### System Shutdown

Table 4 provides the system shutdown procedures for the Genesis2 servers.

Table 4: System Shutdown

|  |  |  |
| --- | --- | --- |
| **Component** | **Procedure** | **Additional Comments** |
| Apache Server | sudo service httpd stop | TBD |
| Genisis2 Application Wildfly Server | ps -ef | grep jboss | awk '{print $2}' | xargs kill -9 | TBD |

#### Emergency System Shutdown

For an emergency system shutdown, Table 5 lists the system shutdown procedures for the Genesis2 servers.

Table 5: Emergency System Shutdown

|  |  |  |
| --- | --- | --- |
| **Component** | **Procedure** | **Additional Comments** |
| Apache Server | sudo service httpd stop | TBD |
| Genisis2 Application Wildfly Server | ps -ef | grep jboss | awk '{print $2}' | xargs kill -9 | TBD |

### Back-up & Restore

Figure 1 represents the Genisis2 server architecture. It consists of the following components that need to be backed up:

* Apache Webserver running Red Hat Enterprise Linux (RHEL)
* Apache Webserver2/Wildfly Application Server running RHEL
* Database Server running Microsoft Windows 2008 R2, SQL Server 2012

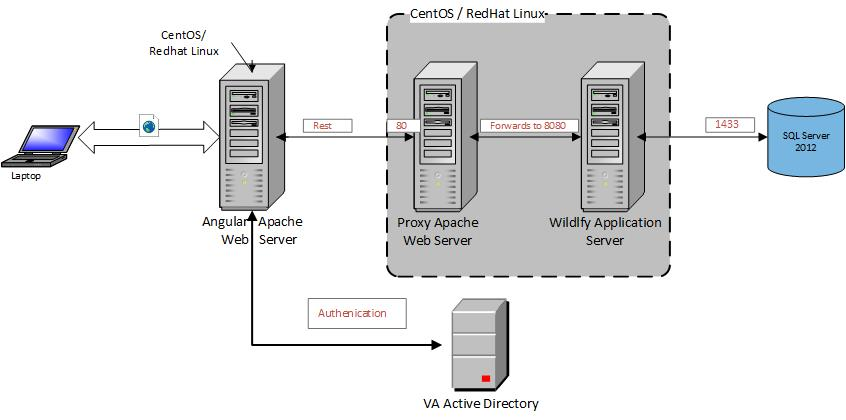


Figure 1: Genisis2 Server Architecture

#### Back-up Procedures

Table 6 provides frequency recommendations for performing back-ups. Veterans Affairs (VA) Enterprise Operations (EO) follows their Standard Operating Procedures (SOPs) for completing the back-ups.

Table 6: Component Back-up Frequency

|  |  |  |
| --- | --- | --- |
| **Category** | **Component** | **Frequency** |
| Applications | Applications | Daily back-ups |
| Application Servers | Apache Web Server  Application Server  Build Server | Weekly full back-ups |
| Database | Database | Hourly back-ups |
| Database Server | Windows Data Base Server | Weekly full back-ups |

#### Restore Procedures

Restore procedures from back-ups may be necessary. Depending upon what needs to be backed up, VA EO follows their existing SOPs for completing the restores.

Table 7 lists the applicable back-up frequency from which restores can be performed.

Table 7: Component Restore Frequency

|  |  |  |
| --- | --- | --- |
| **Category** | **Component** | **Frequency** |
| Applications | Applications | Daily back-ups |
| Application Servers | Apache Web Server  Application Server  Build Server | Weekly full back-ups |
| Database | Database | Hourly back-ups |
| Database Server | Windows Database Server | Weekly full back-ups |

#### Back-up Testing

Recommendations for back-up testing include performing a restore operation. Specifically:

1. For applications – follow the standard EO restore procedures for Linux servers.
2. For database – follow the standard EO restore procedures for the Microsoft SQL server 2012 and the Windows server.

#### Storage and Rotation

Recommendations for storage and rotation are that EO follows their standard disaster recovery procedures currently in place.

## Security / Identity Management

Figure 2 represents the Genisis2 security architecture.



Figure 2: Genisis2 Security Architecture

User Names and Passwords are controlled by centralized VA LDAP access control processes. Password Expiry and other administrative processes are controlled by VA LDAP group.

Genisis2 uses integrated PIV/Windows Authentication that the VA LDAP server supports. When a user logs into the VA Network using their PIV card, they are authenticated initially. Genisis2 uses browser-based Windows Authentication to authenticate the login of this user and then uses Genisis2 Roles to allow access to parts of the Genisis2 application. If a user does not have a role within Genisis2, they cannot proceed beyond the login page. Genisis2 user types are managed by the Genisis2 application to provide each user with certain functionality, depending upon their role. For example, a user is recognized as a Requestor, Data Destination Manager, Data Source Manager, or Genisis2 System Administrator, and are afforded different levels of functionality within the application.

### Identity Management

Genisis2 supports the following user types:

1. Requestor
2. Data Destination Manager
3. Data Source Manager
4. Genisis2 System Administrator (planned for a future release)

The Requestor has the minimum set of activities they can access and perform in the application. For example, the Requestor can generate and track their own data requests.

The Data Destination Manager has all the capabilities of a Requestor, but can review and approve requests, review and approve data results, and track requests more broadly.

The Data Source Manager addresses any questions about the data that they may have with the Requestor (through the Data Destination Manager and not directly), prepares and places the data in a Source landing zone database, and notifies the Data Destination Manager of its location.

The Data Destination Manager will then copy the data over from the Source landing zone database to the Destination landing zone database, extract the data to a flat file, and perform any additional cleanup that may be required. Personally Identifiable Information (PII) and Protected Health Information (PHI) information is then removed from this data and copied over to the specific Study Mart set up for the Requestor.

The Genisis2 System Administrator is a super user that has access to all of the functions that the Requestor and the Data Destination Manager have; and in addition, the Genisis2 System Administrator can Create, Modify, or Delete users. The Genisis2 System Administrator is responsible for creating a user account within Genisis2 and assigning one of the roles. The Genisis2 application then coordinates with the VA LDAP server to create and store the role information.

### Access Control

As indicated in Section 2.2, User Names and Passwords are controlled by centralized VA LDAP access control processes. Password Expiry and other administrative processes are controlled by the VA LDAP group.

Genisis2 uses browser-based Windows authentication for username and password authentication. Genisis2 manages user types and provides the user with access to specific functionality as described in Section 2.2.1.

## User Notifications

EO may have specific user notification and escalation protocols for attending to systems that are down with other applications and servers on which they are hosted.

Recommendations for user notifications for any scheduled or unscheduled changes in the system state such as planned outages, patch upgrades, etc. are that EO follows their standard procedures for user notifications/escalations currently in place.

### User Notification Points of Contact

Recommendations for user notifications for any scheduled or unscheduled changes in the system state such as planned outages, patch upgrades, etc. are that EO follows their standard procedures regarding specific notification points of contact (POCs) currently in place.

## System Monitoring, Reporting, and Tools

Recommendations for system monitoring, reporting, and tools are that EO follows their standard procedures for such activities currently in place. These same tools and processes can be used for with Genisis2 servers.

### Dataflow Diagram

The Genesis2 Request flow is depicted in Figure 4.



Figure 4: Genisis2 Request Flow

### Availability Monitoring

Recommendations are that for Genisis2, EO follows their standard procedures for monitoring the availability of other applications, and monitoring the performance of applications for capacity planning purposes.

### Critical Metrics

There are no metrics specific to the Genisis2 application regarding uptime or downtime. EO may have standard uptime metrics in place for monitoring the availability of applications. Our recommendations are to use the same ones for the Genisis2 application.

## Routine Updates, Extracts and Purges

Genisis2 does not and should not require any routine data purges. The application needs to maintain a history of requests from Day 1 and keep them for posterity. The data stored is not so large as to require purges for the near future.

## Scheduled Maintenance

Genisis2 scheduled maintenance requires routine patches for these software components:

* Red Hat Linux
* Microsoft Windows Server 2008 R2
* Microsoft SQL Server 2012

EO can use their standard operating procedures to schedule a maintenance window at a time that is convenient for and in coordination with the user base.

## Capacity Planning

Genisis2 is not such a performance intensive application that it requires periodic capacity planning reviews. The current capacity planned in terms of number of servers, memory, and disk space assigned is more than sufficient to handle over 50 times the current user base expected.

### Initial Capacity Plan

The initial number of users expected over the next two years is a maximum of 100, with no more than 50 users expected to be logged in concurrently. The current capacity planned in terms of number of servers, memory, and disk space assigned is more than sufficient for 3+ years of operation.

# Exception Handling

Recommendations are that EO follows the standard Tier1 and Tier2 support processes currently in place for Genisis2 exception handling that it uses for other VA applications.

## Routine Errors

### Security Errors

Authentication and Authorization errors can be expected. Since Genesis2 uses the VA LDAP system, standard VA Tier 1 and Tier 2 support processes currently in place for the inability to log in because of a wrong password, wrong username, etc. are recommended for Genisis2.

### Time-out Errors

Genisis2 time-out errors may occur when the webserver is not available. Standard VA Tier 1 and Tier 2 support processes currently in place for unavailable applications due to the webserver or network being down are recommended for Genisis2.

### Concurrency

Genisis2 concurrency errors are not expected or identifiable separate from application errors. Standard VA Tier 1 and Tier 2 support processes currently in place for unavailable applications are recommended for Genisis2.

## 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 subsections contain information to aid administrators, operators, and other support personnel in the resolution of significant errors, conditions, or other issues.

### Application Error Logs

The application error logs are located as follows: - /opt/genisis-application-wildfly-10.0.0/standalone/log/server.log

### Application Error Codes and Descriptions

No application specific error codes exist for the Genisis2 application.

### Infrastructure Errors

#### Database

Microsoft SQL Server 2012 is a component of the Genisis2 application. Generic database errors troubleshooting can be found in the Microsoft web pages located at <https://msdn.microsoft.com/en-us/library/aa952081.aspx>. The site discusses typical connectivity, permissions, and database sizing problems. Standard VA Tier 1 and Tier 2 support processes currently in place are recommended for Genisis2.

Genisis2 application errors are manifested as application errors and are covered in the Genisis2 Maintenance and Troubleshooting Guide.

#### Web Server

The troubleshooting guide for the Apache Web Server is located at <https://httpd.apache.org/docs/2.4/custom-error.html>.

#### Application Server

The troubleshooting guide for the JBOSS Wildfly Application Server is located at <https://docs.jboss.org/author/display/WFLY10/Troubleshooting+Common+Issues>.

#### Network

EO manages the network where the servers are hosted for the Genisis2 application. Standard VA help desk operational processes currently in place for addressing network errors are recommended for Genisis2. The Genisis2 application has been configured and tested with a standard set of network parameters. Due to security protocols, any changes in these parameters should be addressed by EO.

* + - 1. **Authentication and Authorization**

User Names and Passwords are controlled by centralized VA LDAP access control processes. Password Expiry and other administrative processes are controlled by that group. (Refer to Figure 2 for the Genisis Security Architecture diagram.)

Genisis2 uses integrated PIV/Windows Authentication that the VA LDAP server supports. When a user logs into the VA Network using their PIV card, they are authenticated initially. Genisis2 uses browser-based Windows Authentication to authenticate the login of this user and then uses Genisis Roles to allow access to parts of the Genisis2 application. If a user does not have a role within Genisis2, they cannot proceed beyond the login page. Genisis2 user types are managed by the Genisis2 application to provide each user with certain functionality, depending upon their role. For example, a user is recognized as a Requestor, Data Destination Manager, or Genisis2 System Administrator and are afforded different levels of functionality within the application.

Errors relating to Authentication and Authorization may lead a user to the VA LDAP, since that group manages the Username/Password authentications for Genisis2. EO or the appropriate VA LDAP help desk would be the authorities that address these errors through the use of Tier 1 and Tier 2 support procedures currently in place.

#### Logical and Physical Descriptions

Refer to Figure 1 for the Genisis2 server architecture diagram.

The Webserver consists of Apache running on RHEL. It employs Angular JS as the User Interface (UI) framework.

The Wildfly Application Server runs on RHEL. It supports two main components: the Application Code in Java and the Java Business Process Management (JBPM) engine.

The Database Server runs Microsoft Windows 2008 R2 and hosts a Microsoft SQL server 2012. The Genisis2 Databases are hosted here.

## Dependent System(s)

Genisis2 acquires the users’ usernames/passwords and other user details from the VA LDAP system. This is the only system Genisis2 is dependent upon and in programmatic communication with automatically. Errors/troubleshooting are handled by the appropriate VA LDAP help desk.

## Troubleshooting

The step by step process for troubleshooting when the system is not up and the users not able to log in:

* 1. Ensure that the Apache and Wildfly servers are up and running.
  2. Ensure that the correct configuration files are present in each server and are pointing to the correct end points.
  3. Ensure that the firewall ports are open and the servers can communicate with each other.
  4. Ensure that the SQL server is up and running and correct access credentials are present (edited).
  5. Ensure that SQL server user has adequate database permissions for CRUD operations.

## System Recovery

EO manages the servers for the Genisis2 application. Standard system recovery processes currently in place should be used for bringing the systems back online. If all servers are back online, then Genisis2 services are also restored. Genisis2 application components communicate using REST calls and were configured and tested with these calls.

### Restart after Non-Scheduled System Interruption

Since EO manages the servers for the Genisis2 application, standard system recovery processes currently in place should be used for bringing systems back online after a non-scheduled system interruption.

### Restart after Database Restore

Since EO manages the servers for the Genisis2 application, standard system recovery processes currently in place should be used for bringing systems back online after a database restore operation.

### Back-out Procedures

The back-out procedures for the Application Server and the Webserver are as follows:

* Wildfly Application Server: Delete the Wildfly War file from deployment directory.
* Apache Webserver: Delete all contents under /var/www/html/.

### Rollback Procedures

Release 1 will be running on the PRE-PROD environment with the database frozen as of the date of Release 2. Follow the installation procedures for Release 1 on the PROD environment. Copy the Release 1 Database from the PRE-PROD database server to the PROD server. This will rollback Release 2 to Release 1 on the PROD production servers. Restart services on the PROD machines.

# Operations and Maintenance Responsibilities

EO manages the network where the servers for the Genisis2 application are hosted. Standard help desk operational processes currently in place should be used for addressing operations and maintenance responsibilities at the data center where the application is hosted. Usually, these include patches for security and routine minor version upgrades for security and performance reasons. If major upgrades are needed, the application may need to undergo a proper version release process with appropriate testing beforehand.

# Approval Signatures

REVIEW DATE:

SCRIBE:

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Program Manager, Ken Rikkard                                                                                           Date

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Product Owner, Saiju Pyarajan                                                                                             Date

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Receiving Organization, Karen Leake                                                    Date

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Product Support, Paul Hsieh                                                                                                 Date

Template Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| March 2016 | 1.6 | Updated to remove PMAS references and to include VIP references. Eliminated unnecessary text and most instances of passive voice. | Wichita VIP Release Process Team |
| June 2015 | 1.5 | Updated cover and edited for Section 508 conformance and remediated with Common Look Office tool | Process Management |
| May 2015 | 1.4 | Revised content by PMAS Process Improvement Lockdown and reordered cover sheet to enhance SharePoint search results | Process Management |
| November 2014 | 1.3 | Updated Section 4 for url change to the Operations and Maintenance Responsibility Matrix | Process Management |
| December 2013 | 1.2 | Correction to headings | Process Management |
| March 2013 | 1.1 | Formatted to documentation standards and edited for Section 508 conformance | Process Management |
| January 2013 | 1.0 | Initial Document | PMAS Business Office |