HP OpenView Select Audit

For the Windows®, HP-UX®, and Linux® Operating Systems

Software Version: 1.01

Concepts Guide

Document Release Date: November 2006
Software Release Date: November 2006

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

HP OpenView Select Audit includes software developed by third parties. The software HP OpenView Select Audit uses includes:

- ANTLR Copyright 2005 Terrence Parr.
- commons-logging from the Apache Software Foundation.
- Install Anywhere, Copyright 2004 Zero G Software, Inc.
- Jasper Decisions Copyright 2000-2006 JasperSoft Corporation.
- JavaScript Tree, Copyright 2002-2003 Geir Landro.
- Legion of the Bouncy Castle developed by Bouncy Castle.
- log4J from the Apache Software Foundation.
- OpenAdaptor from the Software Conservancy.
- Quartz, Copyright 2004 - 2005 OpenSymphony
- spring-framework from the Apache Software Foundation.
- Tomahawk from the Apache Software Foundation.
- treeviewjavascript from GubuSoft.
- Xalan-Java from the Apache Software Foundation.
- Xerces-Java version from the Apache Software Foundation.

Documentation Updates

This manual's title page contains the following identifying information:

- Software version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP OpenView Support web site at:

www.hp.com/managementsoftware/support

HP OpenView online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introduction

HP OpenView Select Audit is part of HP's business service Identity Management Suite. Select Audit provides reporting, monitoring, and alerting capabilities to facilitate risk assessment and breach response processes. It outputs data to multiple destinations including databases and files. Different output destinations can be configured based on the type of audit data, such as audit component (administration session, authentication, access query) and event level (information, warning).

Identity management touches upon almost every aspect of the HP Adaptive Enterprise vision, affecting access to information across hardware, software, network resources, application servers, enterprise applications, and web portals within an organization and across organizations via business-to-business transactions.

HP OpenView Select Audit provides systematic and secure data collection and reporting covering network services and the enterprise resources they support. By using a highly scalable and extensible architecture, Select Audit integrates with most dynamic IT environments including:

- HP's OpenView Select family of identity management applications
- Third-party identity management collection applications

Audience

This document is intended for anyone using or deploying Select Audit either as a standalone access reporting tool or as part of a larger HP OpenView Identity Management solution. It helps you understand important concepts that are part of Select Audit.

The Select Audit Documentation Set

This manual refers to the following Select Audit documents. These documents are installed with Select Audit and are available in the `<install_path>/docs` folder where `<install_path>` represents the path where Select Audit is installed.

- *HP OpenView Select Audit 1.01 Administration Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`administration_guide.pdf`).
- *HP OpenView Select Audit 1.01 Installation Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`).
- *HP OpenView Select Audit 1.01 User's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`user_guide.pdf`).
- *HP OpenView Select Audit 1.01 Sarbanes-Oxley Model Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`sb_model_guide.pdf`)

- *HP OpenView Select Audit 1.01 Concepts Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`concepts_guide.pdf`)
- *HP OpenView Select Audit 1.01 Report Center User's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`rpt_center_guide.pdf`)
- *HP OpenView Select Audit 1.01 Report Designer's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`rpt_design_guide.pdf`)
- *HP OpenView Select Audit 1.01 Report Developer's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`rpt_devel_guide.pdf`)

Online help is available with the Audit Portal.

Chapter Summary

This guide includes the chapters listed in Table 1.

Table 1 Chapter Summary

Chapter	Description
Chapter 2, Select Audit Overview	This chapter describes the overall design and function of Select Audit.
Chapter 3, Select Audit Architecture	This chapter explains the application's architecture and information flow.
Glossary	This chapter defines terms and concepts frequently used in Select Audit.

2 Select Audit Overview

Identity Management (IDM) is a system of business processes that monitor and control access to online applications and information. Included in identity management are the monitoring and protection of collected information, as well as internal self-monitoring processes to ensure that the IDM system itself is secure. IDM solutions are used to administer user identification and authorization, access rights and limitations, passwords, and other associated access controls. There are often strict governmental or corporate compliance and reporting requirements. The consequences of non-compliance include fines, outages, delays, litigation or even jail. As a result, the management and audit of identity and access across disparate systems, processes, services and environments is a business imperative.

This chapter contains the following sections:

What is Select Audit?

HP OpenView Select Audit is part of HP's business service Identity Management Suite. It manages the complete audit lifecycle and simplifies the fulfillment of regulatory compliance requirements. It helps organizations meet corporate governance requirements by providing a consolidated and tamper-aware identity audit trail. Select Audit integrates seamlessly with OpenView products and with third-party applications.

Select Audit provides continuous compliance in reporting, monitoring, and alerting capabilities to facilitate risk assessment and breach response processes. HP OpenView Identity Management components (Select Access, Select Federation and Select Identity) report every administrative action, user change, access request and authorization decision to a centralized audit system that is accessed by Select Audit to provide accurate, configurable, and timely reports. The entries are digitally signed to prevent the tampering of audit records. This allows the accurate recall of identity events that may impact the business. It answers the questions "Who accessed what resources?", "What should they be doing?", and "What did they actually do?".

Select Audit can also integrate with third-party applications through a Client API to record auditable activities, store them securely, and use the data for reports.

Select Audit helps companies comply with privacy legislation by consolidating logs that contain personally identifiable information (PII) into a central storage location that manages access and data retention, according to company policies.

Key Features

Audit Data Collection

Select Audit collects audit data from the following HP OpenView Identity Management applications:

- HP OpenView Select Identity v4.0
- HP OpenView Select Access v 6.1 SP3 and 6.2
- HP OpenView Select Federation v 6.5 and 6.6

Select Audit may also collect data from third-party identity management applications via a Client API.

The collected audit data includes:

- all administrative actions (main, delegated, and self-service administration)
- all administrative change approvals
- all user actions
- all authentication and authorization decisions
- all system component messages and errors

Audit Collection APIs

Select Audit has interfaces that support C++, Java, and web services to allow third-party applications and resources to send audit data to Select Audit via a standardized audit collection method.

Audit Security and Validation

Select Audit's security and validation features include the following:

- signed blocks of audit data, scheduled Data Integrity reports and on-demand Data Integrity reports
- the ability to configure the number of audit entries that make up a block of audit data to be signed
- the ability for administrators to verify the integrity of audit data

Open Standards

Select Audit is a SOAP-based web service. Audit data is transmitted from the Audit Connector application to the Audit Server as structured XML. Data is then parsed into standard relational database tables to enable easy, standardized access to data for custom report generation, and integration with third-party reporting systems.

Monitoring and Alerting

Select Audit can generate alerts based on audit data coming into the system. The following notification methods are used:

- email
- HP OpenView Service Desk (via email)

Administrators can define alert levels, handling instructions, and recipients for alerts according to customer-established policies. Organizations can create custom alerts to include items such as successful logins, failed logins, and attempts to access a restricted resource.

Identity Audit Consolidation

Select Audit manages identity information from Select Identity, Select Federation, and Select Access. It records all user, system and administrative actions, including delegated and user self-managed tasks.

Segregation of Duty

Select Audit supports the segregation of duties. Access to audit data and reporting can be restricted based on the delegated rights, entitlements and context of administrators in Select Identity. “Auditor” level administrators can view all audit data regardless of their delegated management rights. Select Audit also supports the segregation of duty between administrators who can configure audit policies and administrators who can view audit data and generate reports.

Access Control

Select Audit’s Audit Portal enables authentication and authorization via HP OpenView Select Access. For customers who do not have Select Access, Select Audit supports J2EE platform security for authentication and course grained authorization.

Reports

Users can create summary and dashboard-style reports. Reports can be scheduled to run automatically or be run on demand. Users can also create and save customized report templates.

Select Audit comes with 15 standard Select Audit reports. Separate report packs are available for compliance models. In the first release, one compliance report pack, the Sarbanes-Oxley report pack, is available for purchase. Select Audit also supports current Select Identity reports on audit trail data.

Integration with HP OpenView Products

Select Audit supports integration with the HP OpenView Identity Management Suite (Select Access, Select Federation and Select Identity).

Select Audit includes an OpenView Self-Healing Services data collector, for monitoring the status and performance of all of the HP OpenView Identity Management components. Select Audit may log incidents to Service Desk so the Identity Management system can open trouble tickets for problems, self-service actions, and workflow actions for tracking/tracing capabilities.

HP OpenView Select products have specific configuration requirements in order to log to Select Audit. Unless they are configured properly, the Select applications will not log to Select Audit. Refer to the relevant *HP OpenView Select* documentation for more information about configuring the Select applications.

Integration with Third-Party Products

Third-party applications can report data they collect to the Audit Server through a Client API. HP provides users of third-party applications with an XML format which, when used, ensures that transmitted data can be correctly processed. Customers can also write their own Audit Server-resident data normalizer to process data transmitted in native third-party format.

Technical Specifications

The platforms, servers and applications supported by Select Audit are listed in Table 2.

Table 2 Supported Platforms, Servers, and Applications

Operating system support	• Microsoft Windows 2003 • HP-UX 11.23 • Red Hat Linux AS 3.0 • Solaris 9 and Solaris 10 (Audit Connector)
Application and portal servers	• BEA WebLogic Application Server 8.1 SP5
Audit connectors	• HP OpenView Select Identity 4.0 • HP OpenView Select Access 6.1 P3 and 6.2 • HP OpenView Select Federation 6.5 and 6.6
Audit storage and databases	• Oracle 9i • Oracle 10g • Export of audit data to CSV format
Compliance report packs	• Sarbanes-Oxley (Optional)

Architecture Overview

Select Audit consists of the following main components:

- Audit Client APIs
- Audit Connectors
- Audit Server
- Audit Portal

An installation may have multiple instances of any or all components. There is only one database, shared by all instances of the Audit Server.

Client APIs

Select Audit has Client APIs that support C++, Java and web services interfaces for collecting data from third-party applications and resources.

Audit Connector

The agent-based Audit Connector is installed on the same host as the log message generating system, such as the Select Access Validator and/or Administration server, Select Identity, and Select Federation. The Audit Connector has three sub-components:

- data receiver
- persistent storage
- data sender

Audit Server

The Audit Server stores, normalizes, analyzes, and produces reports. The Audit Server consists of the following sub-components:

- Receiver
- Normalizer
- Compliance model
- Report Server
- Workflow Engine

Audit Portal

The Audit Portal is a web interface used to log in and log out of Select Audit, administer and view reports, monitor dashboards, perform report attestation, configure Select Audit, configure access controls, respond to alerts, and define report templates. Select Audit supports the following browsers:

- Internet Explorer 6
- Firefox

Audit Lifecycle

Select Audit performs the following operations:

- It collects messages on client platforms.
- It communicates messages to the Audit Server in a guaranteed way.
- It processes incoming messages (including filtering and transformation).
- It triggers external processes from incoming messages (email).
- It stores messages in a relational database.
- It retrieves and filters data from the data store, based on Select Identity-based delegated administration permissions.
- It produces reports based on filtered data (on demand and scheduled).
- It manages the configuration of message handling.
- It produces a digitally-signed audit trail which includes information about who configured and accessed the audit trail.
- It provides reliable message storage and transmission using extensible client-side collectors when the Audit Server is unreachable.

Figure 1 illustrates the flow of audit data through Select Audit and how the components interact with the data.

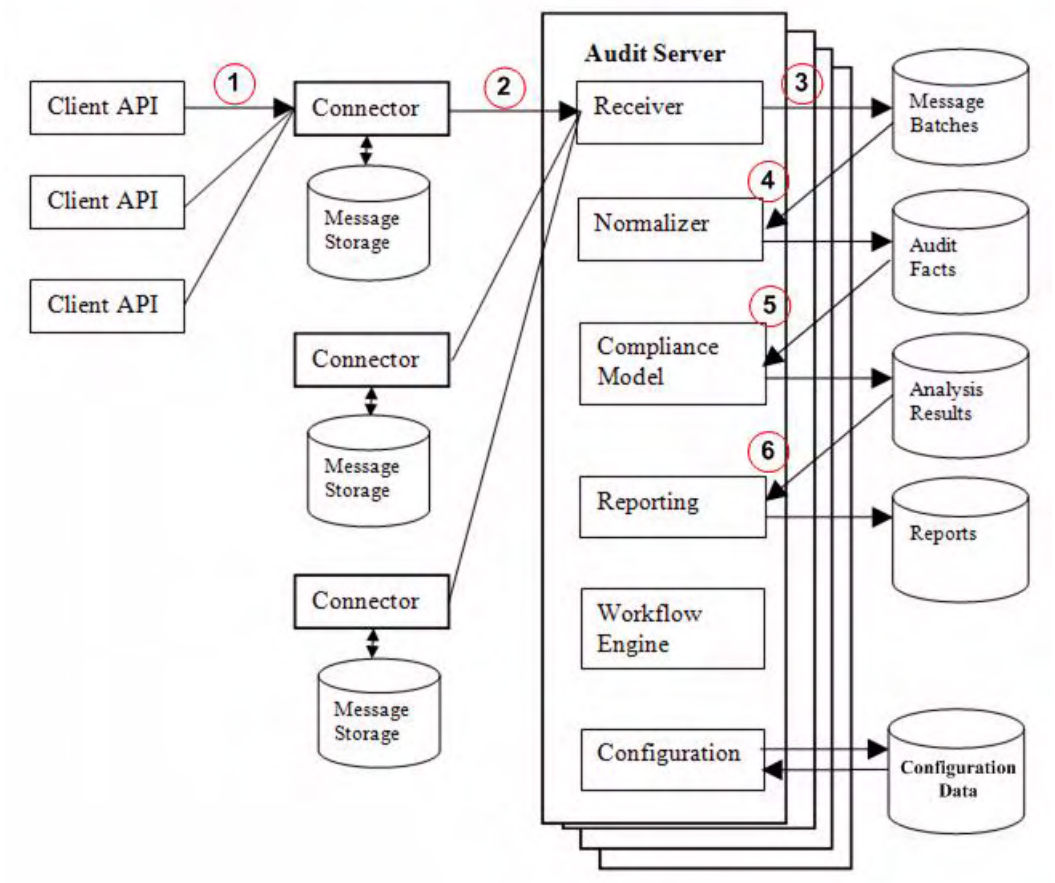

Figure 1 Flow of Audit Data

1. An Audit Client API collects audit messages from an application and sends the messages to the Audit Connector.
2. The Audit Connector receives messages from the audit client and collects audit messages into batches and sends the message batches to the Audit Server.
3. The Audit Server receives the batches from the Audit Connectors and stores the batches in a database.
4. The Normalizer reads message batches from the database, parses them into Audit Facts and creates records in tables with the Audit Facts.
5. The Audit Facts are analyzed by the compliance models. Results of the analysis are stored in the database.
6. The Audit Facts are used to generate reports. Reports are stored in the database and provided to users.

3 Select Audit Architecture

Select Audit is an extensible platform that collects run-time messages from a variety of systems, archives the messages with optional cryptographic integrity protection, and performs analysis and reporting functions on those messages to support both general operations and regulatory compliance processes.

This chapter describes the architecture of Select Audit. It contains the following sections:

Overview

The main components are the Client APIs, the Audit Collector, the Audit Server, and the Audit Portal. Select Audit is implemented in two layers. In the first layer, a generic message handling platform collects messages from message sources, forwards them to the Audit Server, performs configurable processing steps after the messages are received at the server, and supports report generation from stored messages.

The second layer is a specific configuration of the platform with collectors, message processing steps, storage and reports that generate regulation-specific IT Control reports like the reports provided by the Sarbanes-Oxley report pack, based on messages collected from the audit data. The Select Audit architecture is shown in Figure 2.

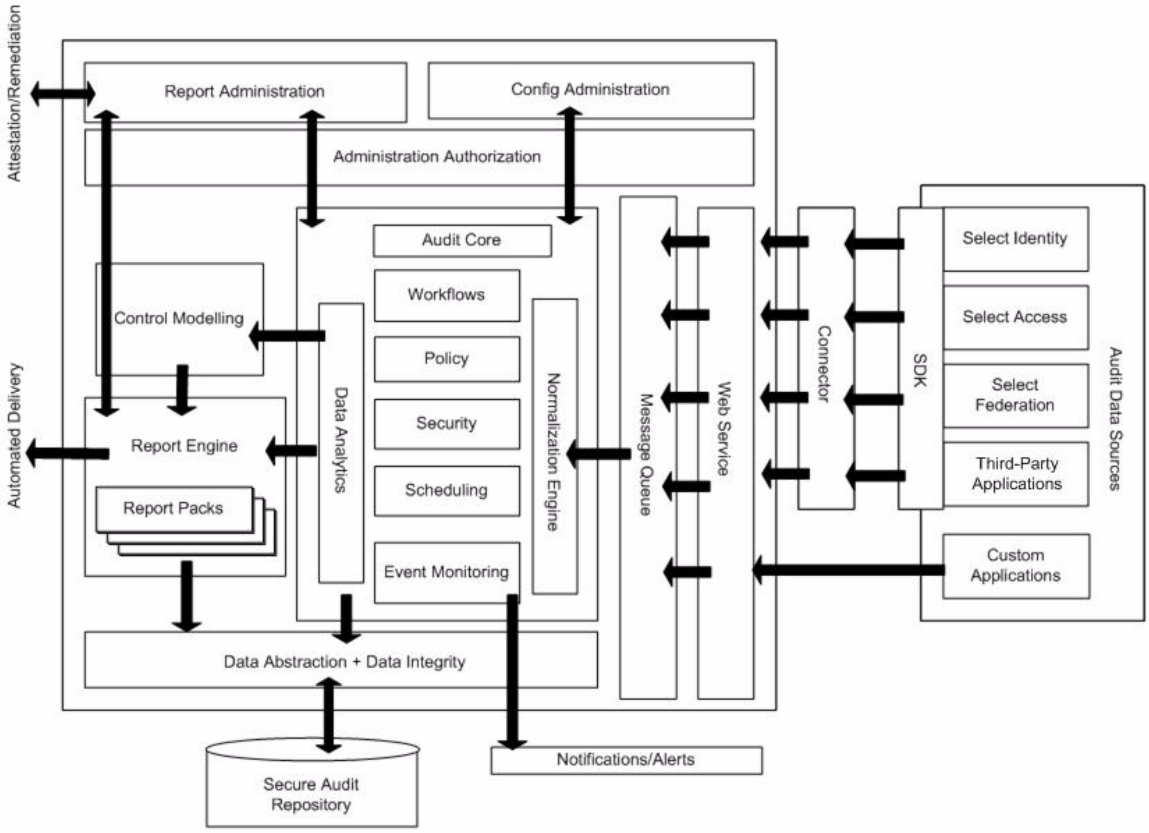

Figure 2 Select Audit Architecture

Message Collection

Messages are logged when the client application sends a message to an Audit Connector using a TCP/IP socket. Communication is synchronous between the Audit Client API and Audit Connector. The process is as follows:

1. The Client Application sends the message it wants to log.
2. The Audit Client API converts the message to UTF-8.
3. The Audit Client API acquires a connection to the Audit Connector.
4. The Audit Client API transmits the message to the Audit Connector.
5. The Audit Client API waits for a reply from the Audit Connector.
6. The Audit Client API returns a result to the client application.

Audit Client APIs

The Select Audit Client API consists of libraries and components provided for the client applications to facilitate audit messages collection. Client applications use this API to forward the messages to the Audit Connectors. There are Client APIs embedded in Select Access, Select Identity and Select Federation. You can also use the Audit Client APIs to collect messages from third-party systems.

All Audit Client APIs have the following features:

- They handle socket reconnects automatically.
- They are multithread-safe.
- They require minimal configuration.
- They have little impact on the performance of client applications under normal conditions.

Select Audit has interfaces that support C++, Java, and web services to allow third-party applications and resources to send audit data to Select Audit via a standardized audit collection methods.

Java Audit Client API

Client applications and components that use the Java Audit Client API include:

- Select Access Administration server
- Select Access Java-based Enforcers
- Select Identity
- Select Federation

The Java Audit Client API is packaged as a Jar file (`selectauditclient.jar`).

C/C++ Audit Client

Client applications and components that use the C/C++ Audit Client API include:

- Select Access Validator
- Select Access C/C++/.NET Enforcers

The C/C++ Client API is part of the `enforcer.dll`. Methods open and initialize a handle to the Audit Client object, log a message using the handle, and cleanup any resources used by the Audit Client.

Third-Party Applications and Client APIs

Third-party applications that capture auditable events can be configured to work with Select Audit. In general, the application should be configured so that only those events that are to be stored, protected, and managed are sent to the Select Audit system. Other events should be trapped and retained within the application and not passed to Select Audit.

The application Call Log function can be configured to call the appropriate Audit Client API (C/C++ or Java). The Client API can send messages to the internal application as well as to the Audit Server. Other function calls are used to log those messages considered relevant.

Audit Connector

Audit Connectors are components deployed on systems running client applications that collect audit messages from the client applications, temporarily store these messages, and send them to the Audit Server. The Audit Connector receives messages from the Client API, queues those messages in a local file stored on the client host, and periodically sends batches of messages to the Audit Server over a secure, authenticated channel. Client messages are encapsulated into a batch using XML. The messages are then sent to the server as the body of an HTTP POST request.

The Audit Connector is a combination of a thin API linked into the client program, and a separate service/daemon that runs on the same host as the client program. Communication between the client and the Audit Connector is over TCP/IP sockets bound to the local host address.

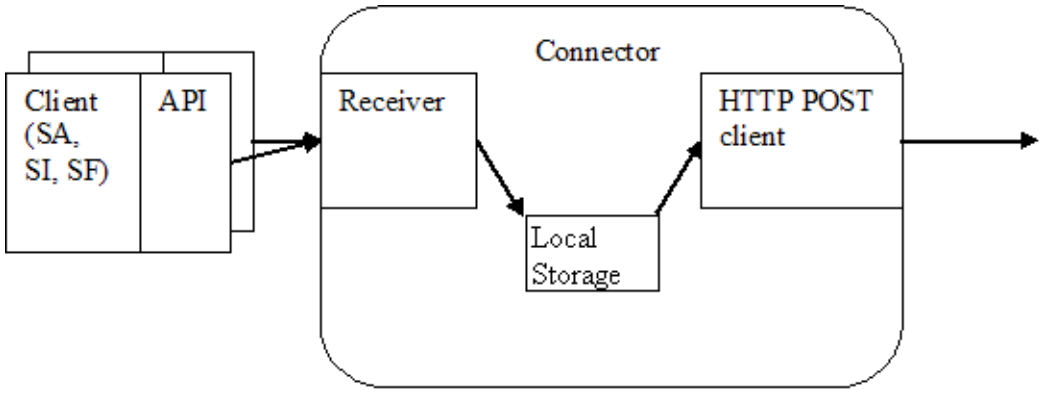

Figure 3 Audit Connector Architecture

Audit Server

The Audit Server is comprised of three general components:

- Receiver
- data analysis and reporting
- server management and configuration

These components work together according to the following synopsis:

1. Batches of audit messages arrive from the Audit Connectors.
2. The Receiver stores the message batches in the database. After storing the data, the data receiver triggers the normalization component.
3. The message batches already stored in the database are transformed into database tables suitable for creating reports.
4. The reporting component performs workflow-related activities such as sending alerts and obtaining approvals for reports. The transformations and workflows are described by the reporting model, which is a tree of requirements necessary to demonstrate compliance with regulation control objectives.

5 To transform the data, the model is first decomposed into the message processing rules which drive the message processing engine.

6 The Audit Server's components and configuration are managed through the Audit Portal.

The overall architecture of the Audit Server is shown in the following diagram:

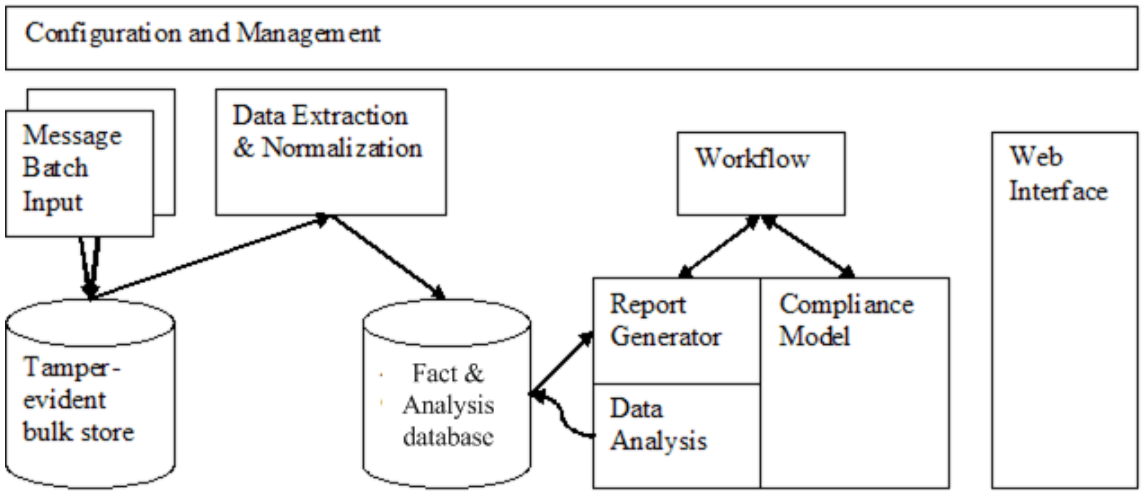

Figure 4 Audit Server Architecture

The batch input, bulk message storage and data extraction sections collect incoming messages, and convert those messages to standard relational tables. The data is extracted to other standard relational tables for data analysis and reporting.

Message Receiver

The Receiver receives incoming message batches from the Audit Connectors, performs data integrity protection, and stores the batches to standard relational database tables. When a batch of messages is received, it commits the batch to the tamper-evident bulk store and then returns a success indicator to the client.

The Audit Connectors opens long-lived HTTP(S) connections to the Audit Server, using SSL. Messages are collected from Select Access (from both the Validator and the Administration server), Select Identity and Select Federation and, potentially, other sources. On the Audit Server, a pool of servlets waits for HTTP requests from the Audit Connectors. Once the data is received, the Receiver sends an HTTP response to the Audit Connector.

- Messages are not permanently removed from the incoming queue until all the processing is complete.
- Messages that are never selected, or fail during transformation are stored in an Exception table.

Tamper-Evident Bulk Store

The Audit Server calculates a secure hash of each message batch, chains the hashes together to detect missing batches, and timestamps the hashes so that tampering can be detected. The batch is stored in the relational database, along with all relevant hash information.

Normalizer

The data extraction module takes raw batches and extracts the information for Select Audit reports. The extracted information is stored in database tables for analysis by Select Audit and by external tools.

The Normalizer reads message batches from the database, parses them into Audit Facts and creates records in database tables. Each audit message can be normalized into many rows and columns in many Fact tables.

- The server instance that normalizes a message batch may not be the same instance as received and stored the batch. As a result, message batches could be normalized in a different order than received.
- The extraction and normalization modules may be extended or replaced as necessary, to support new applications or reports.

The Normalizer is designed to handle the XML format of incoming message batches from Select Identity, Select Access, and Select Federation automatically. Third-party applications that follow the HP-provided XML specification are automatically handled as well.

- If a third-party application transmits its message batches in its native format, a special Normalizer must be written to handle this format.

Transformations are performed to enrich the data with additional information which consists of the following:

- a batch ID
- a batch arrival timestamp
- the security principal's name
- the Audit Connector authentication type
- the Audit Connector's remote user name
- the Audit Connector's remote address
- the Audit Connectors' remote port number
- the URI of the Audit Server's resource
- the parameters of the resource request

The Audit Facts are then extracted to standard relational tables for analysis.

Compliance Model and Data Analysis

Users interact with Select Audit through a dashboard that presents information based on a compliance model. A compliance model is built from a high-level view of the business processes, regulations, and audit control points. The model is then linked to the actual data, providing a structured compliance dashboard that matches the business processes. A Workflow Engine is tied to the compliance model and reports. The Workflow Engine implements alerts, the attestation of report content, and similar activities.

The Audit Facts are analyzed to determine and update the state of the compliance model. The compliance model:

- gets a subset of Audit Facts from the database
- analyzes the Audit Facts
- builds database tables with the results of the analysis (the state of the model)
- generates reports with a visual representation of the model's state
- stores the generated reports in the database
- starts workflows to send alerts and notifications

The compliance model has a tree structure that users can drill down through to view increasing level of details of the model's state.

Some users may be allowed to enter into only some fragments of the tree.

Model analysis is run every 24 hours at 2:00 am to provide a current dashboard of the state of adherence to compliance controls. The status is shown as green, yellow, or red. The trend indicates better than previous, similar to previous, or worse than previous periods.

Results of the analysis are stored in the database and are used to generate reports on the state of compliance and to send notifications about events. The stored Audit Facts are also used to generate reports on audit data.

The model report configuration file and the analysis output information are used to generate web pages that display the status of the model to users.

Data Analysis Engine

The Data Analysis Engine invokes data analysis plugins, based on rules generated from the compliance model. Data analysis plugins:

- transform database tables with audit data into other tables
- create user readable reports from the database tables, using predefined templates
- send alerts
- send reports for attestation and approval

The Data Analysis Engine is run every 24 hours at 2:00 am. Data analysis is performed in two phases:

- It generates intermediate database tables and reports.
- It performs workflows.

The intermediate tables are signed to make them tamper-evident. The signature algorithm is incremental so adding records to a table does not require resigning the entire table. The newly-added records are chained to the signature of the records already in a table.

Workflows

Select Audit uses the same type of workflows as provided with Select Identity. The Workflow Engine is linked to the compliance model and the Report Generator, and may also be used as part of alerting. Workflows are started from the compliance model, or other models, based on the state of the model. The reporting component performs workflow-related activities.

The Workflow Engine implements alerts, sends out audit reports for attestation and accepts attestations of reports. The Workflow Engine reads workflow definitions from the database and updates workflow state data.

The Notification Workflow steps are shown in Figure 5.

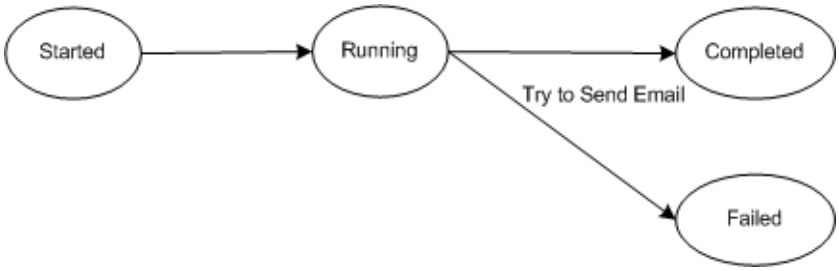

Figure 5 Notification Workflow Steps

The Attestation Workflow steps are shown in Figure 6.

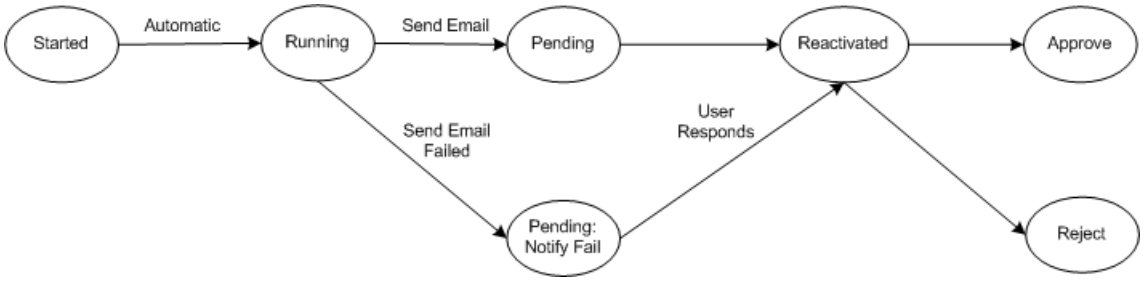

Figure 6 Attestation Workflow Steps

Reporting

Select Audit's reporting capabilities enable organizations to define reports and reporting procedures to meet their operational and audit policy needs. Authorized administrators can create, view, save, and print reports on identity and access administration and user actions. Reports can be sorted and/or filtered by any audit data including users, servers, administrators, dates, specific events, and custom data.

Select Audit's reporting module provides a professional package that includes a report designer, access control and data filtering features, charting and report drill-down capabilities, scheduling, flexible data sources, and multiple output formats. Also included are 15 pre-configured Select Audit reports that can be used as provided or customized for specific reporting requirements.

A Sarbanes-Oxley report pack can be purchased as an add on.

Report Center

The Report Center is the web-based interface of the Report Server that is used to view, print, and export reports. The Report Center is accessed via the Audit Portal. The Report Center lets you manage reports and catalog items in the Library. Using the Report Center, you can:

- run reports
- view pre-run report output
- browse through the Library
- upload and publish reports to the Library
- create and edit report schedules
- set permissions for reports and Catalog items
- unpublish and delete reports from the Library
- administer the view of the Library by specifying a preferred language, a preferred Report Center view and commonly-run reports

Select Audit Reports

Select Audit comes with standard Select Audit reports that can be used as provided or can serve as the basis for customized reports. These reports are categorized according to usage and contents. Data items may appear on more than one report.

The Select Audit Reports folder contains 15 predefined Select Audit Reports, as listed in Table 3:

Table 3 Select Audit Reports

Report Name	Details
Account Change Report	Contains all user account change actions (add, delegate, change, etc.).
Account Events Report	Contains all account event actions (security violations, admin login errors, expired passwords, etc.).
Administrator Report	Contains all administrator actions (configuration changes, authentication changes, password resets, etc.).
Attestation Report	Contains all attestation actions (approved, pending, denied).
Change History Report	Contains administrative audit as complete tasks (the action initiated on this date by this user at this time, approved first by this person at this time, approved next by this person at this time, and the change took affect at this time).
Configuration Report	Contains all configuration change actions (add, change, etc.).
Data Integrity Report	Contains a list of tampered records IDs and tampered signature record IDs, with change actions (added, modified, removed).
Password Management Report	Contains all password administration actions (expire, logon, etc.).

Table 3 Select Audit Reports (cont'd)

Report Name	Details
Raw Message Report	Contains raw audit messages that aren't normalized through the standard process.
Security Events Report	Contains all security events (security violation, configuration changes, etc.).
Service Report	Contains configuration changes to Select Identity services.
System Activity Report	Contains all system activities (login, logout, changes made, etc.).
User Activity Report	Contains all user activities (login, logout, changes made, etc.).
User Summary Report	Contains a summary of user activities.
Workflow Events Report	Contains all workflow event messages.

Data Integrity

Audit data is protected as soon as the data is collected by Select Audit and remains protected until the data leaves Select Audit as reports or notifications.

Audit data is protected when it is permanently stored in the database. Any temporary data that is stored for a short term is not protected.

The data protection mechanism covers:

- message batches received by the Audit Server and stored in the database
- Audit Facts created by the Audit Server from the audit messages and stored in the database

When Select Audit is installed, data integrity protection is initially disabled. You must use the Audit Portal to load the time-stamping key and enable data integrity protection. See the *HP OpenView Select Audit 1.01 Administration Guide* for more information.

Audit records are digitally signed so that they are tamper-aware. The audit signing is chained to provide a security check across the entire audit system, and segmented to allow the verification of the integrity of a portion of the audit data. The Audit Server calculates a secure hash of each message batch, chains the hashes together to detect missing batches, and timestamps the hashes so that tampering can be detected. The batch, along with all relevant hash information, is stored in the relational database.

Select Audit also audits its own data, including all audit policy configuration changes and all operational tasks such as report creation, report viewing, audit validation, and alerting.

Time-Stamping

An embedded time-stamping service is included in each instance of the Audit Server. The Audit Server does not call the time-stamping service after every batch of audit data because generating time-stamps is costly in terms of network and/or CPU resources. The frequency is

configurable using the Audit Portal and can be based on time or on the number of batches. See the *HP OpenView Select Audit 1.01 Administration Guide* for more information. The time-stamping service is also invoked to verify time-stamps.

The Audit Server uses a public/private key pair to generate time-stamps. Users must supply the key pair when deploying the Audit Server. Select Audit uses the Java keystore. Users are responsible for creating and managing the keystore.

You can change the time-stamping keys, for example, if the private key becomes compromised. If the key is changed, refresh each of the old time-stamps using the new key. You can discard the old private key but the old public key must be kept in order to verify the old time-stamps.

Compliance Model Data Integrity

The state of the compliance model is evaluated periodically, as new Audit Facts appear in the database. Evaluation of the model's state is incremental. The model analyzes a subset of the Audit Facts that arrived after the time of previous evaluation and verifies the integrity of query results. The Audit Facts are analyzed, the results are stored in database tables, and the state of integrity of the Audit Facts is propagated to the analysis results.

The analysis results are stored as multiple rows in multiple tables. The integrity protection mechanism is the same as for Audit Facts. Only the results that are permanently stored are protected; temporary values are not protected. Since the analysis is incremental, the output data may already exist and must be updated. In such cases, the integrity of already stored results is verified before updating. The model may keep its old results of analysis to show trends. Old results are hash chained to the current results, using time-stamps.

The Audit Server runs a data verification process at a user's request. It can be triggered via the Audit Portal's Administration menu and it evaluates the entire database by verifying the hash chains of Audit Facts collected between a start and an end date. The state of the integrity of Audit Facts is shown in a Data Integrity report that is automatically created by the system at the end of the verification process.

The Data Integrity report shows the result of the data integrity verification allowing the user to see three types of errors: data errors, signature errors, data not signed errors. The user can also drill down to see the details of each type of error.

The analysis results are used to render reports about the state of the compliance model and to send alerts and notifications about events. When a model generates reports on the state of the model, the integrity of analysis results are verified.

Reports have a tree structure similar to the structure of the analysis modules. The integrity of stored reports is protected.

Report Server Data Integrity

The Report Server queries the database for a subset of Audit Facts, in the same way as the compliance model, except that the data is filtered through user permissions. The query results include the time-stamps of each hash chain fragment included in the results. The fact signatures, the chain fragments, and the time-stamps are verified by the Report Server. The subset is stored in database tables, together with the subset's redactable signature.

The rendered reports, together with their signature, can be stored in the database and the integrity of stored reports is protected. When the server sends a stored report to a user, the integrity of the stored report is verified.

Data Integrity Verification

Data integrity is triggered by the user via the Audit Portal. The Data Integrity report is created at this time and contains one row for each verification result. The audit data can be verified in two ways:

- Verification of a subset of data when the database is queried for subsets. The query results are verified against the signatures. Only the results are verified. There is no verification if data not included in the results was deleted or changed, preventing the data from being included in the results. There is no verification if data used to calculate aggregates was attacked. Query results consisting of Audit Facts and their signatures can be attached to reports as a proof of report validity.
- Verification of all data in the entire database or in a time period. This is can be scheduled or done on demand. A Data Integrity report is generated.

The verification of query results is done by the same component that performs filtering of results based on user permissions.

Verification of all the data can be done in the following ways:

- periodically, scheduled from the Audit Portal
- periodically, scheduled as the generation of a Data Integrity report
- on demand, i.e. before the generation of each report

Select Audit provides on-demand verification from the Audit Portal where you can enter the time period for which the data should be verified. If the time period is not entered, the entire database is verified. The verifier stores the results of verification in the database. A Data Integrity report is generated from the results and may be sent via email to administrators.

Select Audit does not provide any support for resigning the data. Select Audit only signs and verifies data that is stored long term.

Authentication and Authorization

Security is provided by one-way authentication of the Audit Connector by the Audit Server with user ID and password. Additional authentication is also provided by the Connector login name/password. The Audit Server authenticates each Audit Connector to determine the unique connector identity. Audit Connectors are installed using SSL as the connection to the Audit Server on the application server in which the user password is encrypted in a recoverable format and stored in the Connector start up properties.

Each component of Select Audit enables security which is provided through either Select Access or basic application server security. By default, no security is implemented for the components. Users must setup security using Select Access or application server default security.

Authentication with the application servers' authentication methods is limited to user ID and password while Select Access allows for a broader range of authentication methods through its authentication servers as well as support for SSO (single sign on). If they are not enforced by Select Access, web-facing resources (including the Receiver), are enforced by the application server using deployment descriptors (`web.xml`).

There are three advantages to securing the Audit Server with Select Access:

- single sign-on
- more authentication methods at the user's disposal, e.g. Radius, NTLM, securID
- simple setup

The Select Access BEA WebLogic Enforcer used to protect Select Audit contains three components:

- authentication Provider using JAAS
- authorization Provider
- Identity Assertion used for SSO or login to other resources on the same server

For more information regarding the WebLogic Enforcer, see the *HP OpenView Select Access Integration Paper for BEA WebLogic™ 8.1 Servers* and the *HP OpenView Select Access Integration Paper for BEA WebLogic™ 9.1 Servers*.

Report Filtering

Report filtering uses a JDBC proxy that uses the user's identity to filter out the report data that the user is not entitled to view. The user credentials are passed to the JDBC proxy using the J2EE Subject. The JDBC proxy performs user authentication, authorization, and report content filtering, using Select Access or J2EE security.

Glossary

A

Access Control

The methods to control access to report data. Report Level control determines which reports are viewable and Row Level control determines which audit events are listed in a report. Access Control also refers to control over access to the Audit Portal.

Ad Hoc Wizard

A report authoring tool for creating new reports. It is accessed using the **Ad Hoc** button in My Reports, in the Report Center.

Admin Dashboard

Component used to perform administration tasks in the Report Server. It is only available to users with administration privileges.

Attestation Workflow

Used to specify the schedule for report approvals and the persons responsible for approving reports.

Audit Connector

Receives messages from the client and sends batches of messages to the Audit Server in a guaranteed fashion.

Audit Facts

The records created as a result of normalizing message batches. They are stored in the database.

Audit Data

Data collected by the client that is of interest to auditors and compliance managers.

Auditor

A person who examines an organization's financial or other policy-related records and reports. Known as an internal auditor if the person is an employee of the organization being audited and an external auditor if the auditor is not an employee of the organization.

Audit Portal

The web portal used to perform the tasks in Select Audit.

Audit Message

Messages collected by the client containing audit data.

Audit Server

The Audit Server receives data from the Audit Connector, normalizes the data, stores the data, performs analysis on the data, and generates reports.

Audit Trail

A chronological sequence of audit records that are used to track computer activity, such as who has accessed a computer system and what operations were performed during a given period of time.

Authentication

Method for determining whether someone or something is who or what it is declared to be.

Authorization

Method for determining whether a person has the required permissions to access systems and what privileges they have within it.

B

There are no terms that begin with this letter.

C

Client API

The libraries and components provided for the client applications to facilitate audit message collection. The Client API is used to forward messages to the Audit Connector.

COBIT

Control Objectives for Information and related Technology. A set of best practices for IT management created in 1992 by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI).

Compliance

Ensuring the Identity Management processes have adequate controls for managing access to financial and other applications and ensuring security is monitored. It also involves Incident Management processes to prevent intruders from gaining access to financial applications.

Compliance Management

Systems for managing compliance requirements.

D

Data Integrity

Methods for verifying that data hasn't been tampered with.

Data Normalizer

See Normalizer.

Data Receiver

The component that receives audit messages from Audit Connectors and securely stores that data.

Data Verification

Data can be verified as not being tampered with by running a scheduled or on demand report. *See* Data Integrity.

E

There are no terms that begin with this letter.

F

Filtering

Select Identity data is filtered so that the same access permissions are applied in Select Audit. Users can only see the Select Identity reports and data they have permission to see in Select Identity.

G

There are no terms that begin with this letter.

H

There are no terms that begin with this letter.

I

Identity Management

A system of processes that monitor and control access to online applications and information.

J

There are no terms that begin with this letter.

K

Key Performance Indicators (KPIs)

Measures used to determine the level of compliance and the effectiveness of the controls.

L

There are no terms that begin with this letter.

M

Message Batches

A collection of audit messages sent to the Audit Server from the Audit Connector.

Model

A means of capturing relationships between controls and how the controls are analyzed for compliance. It reflects the critical processes and indicators for assuring compliance.

Model Threshold

The settings that, if exceeded, trigger Workflow Alerts.

My Reports

The area of the Report Center where users save frequently-viewed and customized reports.

N

Normalizer

The component that parses messages into Audit Facts and creates records in database tables.

O

There are no terms that begin with this letter.

P

There are no terms that begin with this letter.

Q

There are no terms that begin with this letter.

R

Report Center

The part of the Audit Portal used to access reports. Reports can be viewed, printed, scheduled and administered.

Report Designer

The graphical tool used to build and modify reports.

Reporting Engine

The part of the Report Server that is used to define reporting procedures according to operational and audit policies. *See* Report Server.

Report Library

The area of the Report Center containing the available reports.

Report Server

A separate web application consisting of the Admin Dashboard, Report Center and SOAP server. It stores report files in the database library.

S

Segregation of Duty

The restriction of access to audit data and reports, based on rights and entitlements, in relation to other, conflicting rights and entitlements.

Select Access

HP OpenView Identity Management software for secure access control to IT services and resources.

Select Audit Reports

The pre-defined reports that come with Select Audit. Additional report packs can be added.

Select Federation

HP OpenView product that enables web single sign-on and cross-domain identity management without requiring a centralized data repository or repository synchronization.

Select Identity

HP OpenView product that allows centralized management of user identities and access rights over the entire lifecycle.

T

There are no terms that begin with this letter.

U There are no terms that begin with this letter.

V There are no terms that begin with this letter.

W There are no terms that begin with this letter.

X There are no terms that begin with this letter.

Y There are no terms that begin with this letter.

Z There are no terms that begin with this letter.

Index