EVIDEN

Identity and Access Management

DirX Audit

Introduction

Version 7.2, Edition June 2025

Table of Contents

Preface

This manual describes the DirX Audit architecture and components. It consists of the following chapters:

- Chapter 1 provides information about managing audit and compliance with IAM.
- Chapter 2 provides a DirX Audit overview.
- Chapter 3 provides a glossary.

DirX Audit Documentation Set

DirX Audit provides a powerful set of documentation that helps you configure your audit server and its applications.

The DirX Audit document set consists of the following manuals:

- *DirX Audit Introduction*. Use this book to obtain a description of DirX Audit architecture and components.
- *DirX Audit Tutorial*. Use this book to get familiar quickly with your DirX Audit installation.
- *DirX Audit Administration Guide*. Use this book to understand the basic tasks of DirX Audit connectivity administration.
- *DirX Audit Manager Classic Guide*. Use this book to obtain a description of the DirX Audit Manager Classic user interface provided with DirX Audit.
- *DirX Audit Manager Guide*. Use this book to obtain a description of the DirX Audit Manager user interface provided with DirX Audit.
- *DirX Audit Command Line Interface Guide*. Use this book to obtain a description of the command line interface provided with DirX Audit.
- *DirX Audit Customization Guide*. Use this book to customize your DirX Audit environment.
- *DirX Audit History Synchronization Guide*. Use this book to obtain information about the DirX Audit History synchronization jobs.
- *DirX Audit Best Practices*. Use this book to obtain guidelines and tips for avoiding common mistakes and improving the experience of a DirX Audit installation.
- *DirX Audit Installation Guide*. Use this book to install DirX Audit.
- *DirX Audit Migration Guide*. Use this book to migrate DirX Audit from previous versions.
- *DirX Audit Release Notes*. Use this book to understand the features and limitations of the current release.
- *DirX Audit History of Changes*. Use this book to understand the features of previous releases.

Notation Conventions

Boldface type
In command syntax, bold words and characters represent commands or keywords that must be entered exactly as shown.

In examples, bold words and characters represent user input.

Italic type
In command syntax, italic words and characters represent placeholders for information that you must supply.

[ ]
In command syntax, square braces enclose optional items.

{ }
In command syntax, braces enclose a list from which you must choose one item.

In Tcl syntax, you must actually type in the braces, which will appear in boldface type.

|
In command syntax, the vertical bar separates items in a list of choices.

...
In command syntax, ellipses indicate that the previous item can be repeated.

install_path
The exact name of the root of the directory where DirX Audit programs and files are installed. The default installation directory is *userID_home_directory*/**DirX Audit** on UNIX systems and **C:\Program Files\Atos\DirX Audit** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathnames is represented by the notation *install_path*.

install_media
The exact path where the DirX Audit installation media is located.

1. Managing Audit and Compliance with IAM

Identity and access management (IAM) combines business processes, policies and technologies for defining, managing, monitoring and controlling access to IT systems, resources and information by internal and external users.

IAM solutions benefit the virtual enterprise by:

- Improving IT security and risk management
- Helping to ensure regulatory compliance
- Reducing the cost of administration and day-to-day operations
- Improving processes and service-level agreements
- Enhancing business agility and profitability

1.1. The Cornerstones of IAM

IAM solutions provide four distinct functions for managing users and their access rights: administration, authentication, authorization, and audit.

Administration is the process of managing digital identities and their entitlements to systems, applications and resources in the heterogeneous IT environment based on user roles and business rules and monitoring entitlement assignments for compliance to regulatory requirements and business policies. Identity and entitlement administration is provided by the identity management component of an IAM solution, providing an enterprise-wide, cross-platform, centralized and automated user management and provisioning system for the virtual enterprise.

Authentication is the process of identifying users and verifying their digital identities. It includes **identity federation**, which is the set of trust agreements, policies and processes that enable the authentication of identities across enterprise boundaries to build virtual business communities among autonomous organizations.

Authorization is the process of determining whether a user is allowed to access a particular resource. Authentication and authorization comprise the access management component of an IAM solution, providing real-time enforcement of security policies across the IT infrastructure.

Audit is the process of producing, collecting, cleansing, and correlating data about administration, authentication and authorization events and then transforming this data into actionable intelligence with respect to compliance regulations, business security policies and corporate risk management objectives. Audit in an IAM solution is called **identity audit** and provides the means to analyze and report on IAM functioning and deliver the information necessary to support IAM governance.

Identity audit includes the processes that:

- Automatically log the activities associated with identity administration and real-time enforcement of access rights, providing in the generated **audit trail** a chronological sequence of evidence (called **audit messages**) pertaining to and resulting from these operations
- Collect, cleanse, correlate and store the audit trail generated by the IAM activities
- Generate current status about the IAM infrastructure - for example, the access rights a user has today
- Provide for historical analysis of the IAM infrastructure - for example, a snapshot of the access rights a user had last month

1.2. The Challenges of Identity Audit

Identity audit is typically a cross-component solution:

- IAM components automatically produce detailed audit trails of their activities that can be used to demonstrate accountability, while an external audit facility aggregates the audit trails, stores them securely in a central location, and provides the functions for correlating and analyzing the audit trails and reporting on the results to demonstrate control of business processes on user access and entitlements as required by applicable regulations.
- IAM components also provide the functions for generating reports on current status and history on the information in their repositories - for example, the identity store in an identity management component - either automatically or on demand. This information can be brought into the external audit facility for correlation and analysis.

The audit trails and historical data produced by IAM components can help to answer the key questions that auditors ask for proving compliance to IAM controls:

- Audit trails produced by identity management components comprise information about activities on identities, roles, and rules. Analysis of these records can provide information about who requested and approved access rights at what time, who certified the access under which conditions, or which policy permitted the access.
- Audit trails produced by access management components can provide information about
    1. who tried to authenticate to which applications and
    2. who requested access to which resources at what time and
    3. whether or not the authentication and/or authorization was successful.
- Historical data produced by identity management components can provide information about changes to identity and identity-related data over time, allowing for historical review of identities and point-in-time comparisons to demonstrate progressive compliance to governance processes, gain insight into identity and policy status or determine why an access request was permitted.

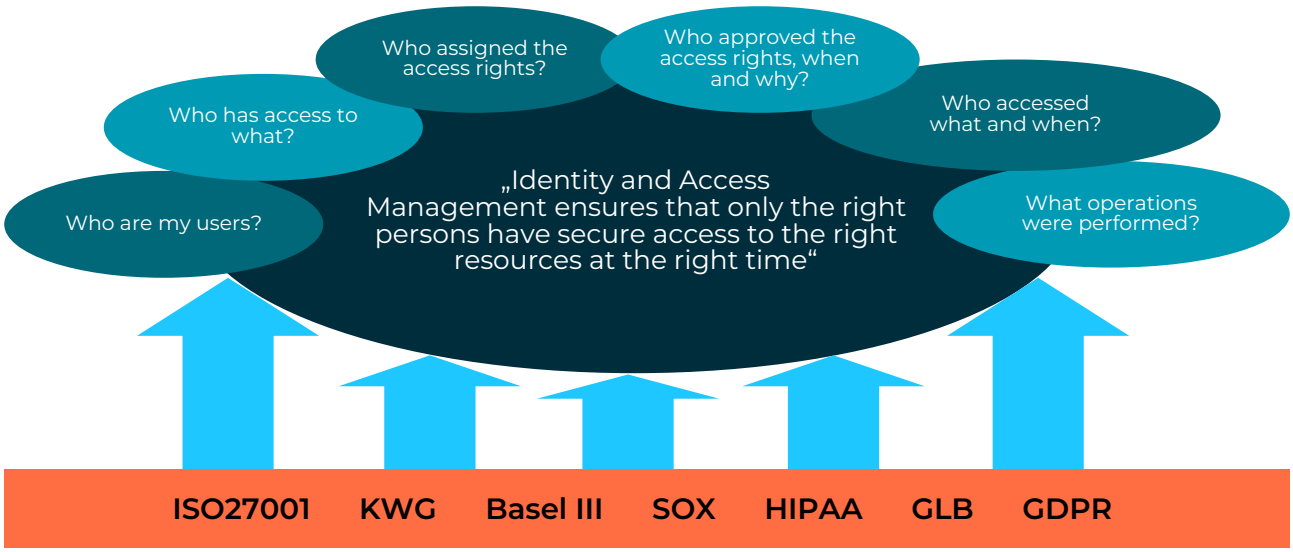

Figure 1. How IAM Supports Audit and Compliance

Identity and access management tools can generate high-quality audit trails. However, reconciling the desired business controls for IAM with the real data provided in the audit trails is not an easy task:

- Different applications and components within those applications use different encoding formats, so audit trail format is different from trail to trail, and the data formats used are not always easy to interpret.
- Users are hard to identify across different audit trails, since the same user can have different IDs depending on the application, and the ID used within the application can change over time.
- Activities in different applications can occur in parallel, so finding the triggering event is often difficult. It is hard to extract a sequential chain of activities of one user among different applications.
- The raw intelligence data provided in the IAM audit trails is not aligned with larger business objectives and corporate regulations, and can take weeks, months or even years to analyze. Auditors need fast and easy access to audit data that can be aggregated and viewed according to key performance indicators (KPIs) for identity audit.

The sheer number and types of regulations also pose a challenge:

- Many different regulations exist today, and new ones are mandated all the time, requiring continuous revision of IAM controls.
- The policy for what is audited depends on the particular regulation, the enterprise business model in force, and the application creating the audit trail, making it difficult to establish consistent, end-to-end audit policies.
- Different regulations require different methods of analysis and reporting and each regulation has its own criteria for analysis and report.

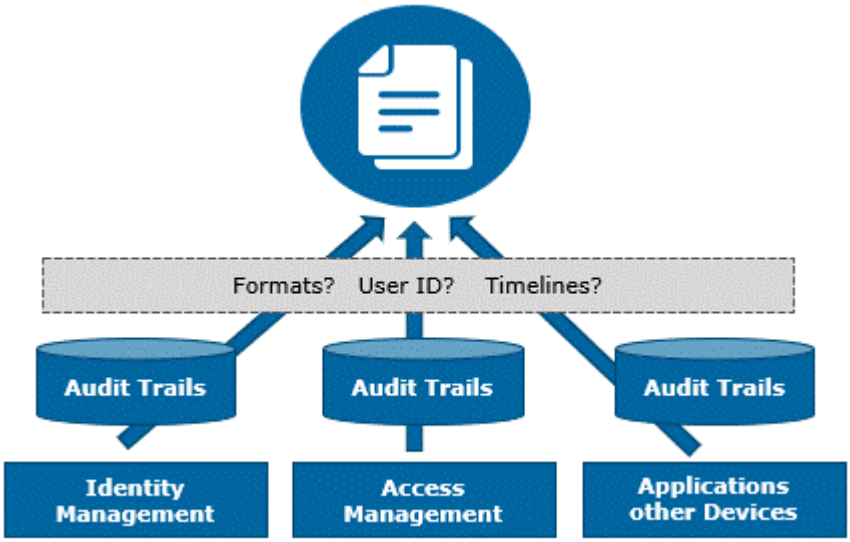

Figure 2. The Challenges of Identity Audit

To address these challenges, an audit facility in an IAM solution needs to provide several features:

- A central, secure audit database that stores the audit trails from all administration, authentication and authorization activities. Using a central repository allows the auditor to analyze the actions of a user throughout the enterprise IT infrastructure instead of on a per-application basis, making security breaches easier to discover and reducing the labor required to report on IAM activities.
- Support for multiple tenants to separate data completely from those of other tenants; especially events and history entries.
- Functions for collecting and normalizing audit data from identity management, access management and other applications to provide a consistent view of audit trails and the sequence of audit messages that comprise them across the heterogeneous IT environment.
- A presentation interface that can aggregate the collected and normalized audit data according to different identity audit-related KPIs and then display the resulting data in a graphic format that auditors can easily view and interpret, allowing them to drill down to details about audited events as necessary.
- A reporting interface that is simple to adjust to evolving regulations and which can be tailored to special customer requirements.
- Fine-grained access control for audit trails and also for specific information within audit trails, to comply with data security and privacy policies mandated by many government, health and financial regulations.

1.3. What is DirX Audit?

DirX Audit is the audit facility offered with the DirX suite for identity and access management solutions. DirX Audit provides a platform for the central collection, normalization, storage, and analysis of audit trails from different IAM audit producers, for centralized, persistent storage of historical identity-related information and a Web-based user interface that facilitates the correlation, analysis and reporting of audit and historical data by auditors, administrators, and security compliance officers. DirX Audit helps to provide the answers to the questions of "who did what, where, when and why" that are so critical to achieving and maintaining compliance, and provides the means to aggregate the vast amount of collected audit data into intuitive and actionable intelligence for input to corporate decision-making and continuous process improvement.

DirX Audit is tightly integrated with the other identity and access management products in the DirX suite. These products include:

- **DirX Identity, for managing who has access to what**. DirX Identity provides a comprehensive, process-driven, customizable, cloud-ready, scalable and highly-available identity management solution for enterprises and organizations. It delivers overall identity and access governance functionality seamlessly integrated with automated provisioning. Features include life-cycle management for users and roles, cross-platform and rule-based provisioning in real-time, Web-based user self-service and delegated administration, request workflows, access certification, password management, metadirectory and auditing and reporting.
- **DirX Directory, for consolidating the storage of digital identities**. DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable and secure LDAP and X.500 directory server and LDAP proxy. DirX Directory can act as the identity store for employees, customers, trading partners, subscribers, and other IoT entities. It can also serve as a provisioning, access management and metadirectory repository, to provide a single point of access to the information within disparate and heterogeneous directories available in an enterprise network or cloud environment for user management and provisioning.
- **DirX Access, for controlling who does what**. DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management and SSO solution providing policy- and risk-based (context-aware) authentication, including FIDO, dynamic authorization based on XACML, and federation for Web applications and services. DirX Access delivers single sign-on (SSO), versatile authentication, including risk-based authentication (also called adaptive authentication), identity federation (based on SAML, OAuth and OpenID Connect), just-in-time provisioning, entitlement management, and policy enforcement for applications and services in the cloud, in IoT environments, and on premise.

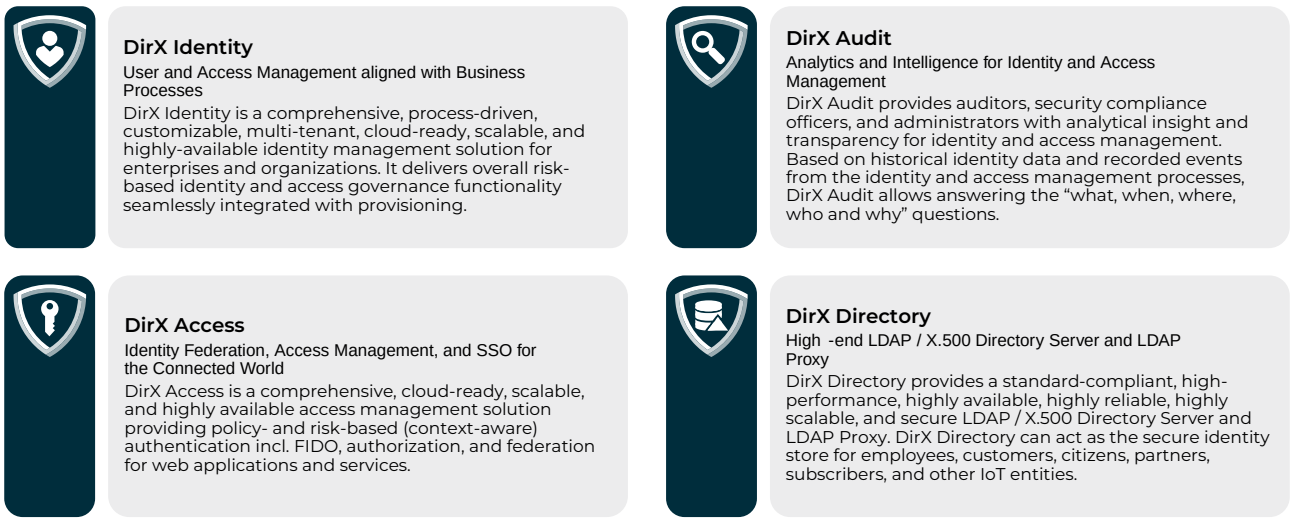

Figure 3. DirX Identity and Access Management Suite

The DirX suite offers a proactive approach to ensuring continuous, sustainable compliance in the virtual enterprise: functions for establishing administrative, authentication and authorization controls are provided in DirX Identity, allowing organizations to establish preventive controls for compliance objectives. For example:

- Metadirectory services allow identities and their access rights to be centrally managed, providing greater transparency into identity management activities and tighter administrative control with fewer administrators.
- Automated role- and policy-based user provisioning ensures that corporate security policies are consistently enforced across all points in the corporate IT infrastructure, avoiding error-prone, ad hoc application of access rights by many different IT administrators working in different parts of the enterprise.
- Approval and re-approval workflows automate the application of corporate authorization policies, ensuring that they are applied consistently rather than on a case-by-case basis, and immediately, rather than as a result of reviewing an audit report. High-risk IAM activities like the assignment of security-sensitive roles can require a client digital signature, providing evidence of the transaction and who authorized it.
- Automated, real-time user de-provisioning ensures that access rights of terminated employees and contractors are immediately and accurately revoked on all affected IT systems.
- Automated reconciliation services can detect suspicious accounts and access rights on corporate IT systems and then eliminate them automatically or report them to the appropriate administrator for handling.
- Segregation of duties (SoD) policies define user-role assignments that violate corporate security policies or create unacceptable risks, and SoD policy enforcement by user provisioning services notifies of any violations that occur for immediate remediation.
- Access certification campaigns allow for periodically checking security-critical user entitlement assignments to ensure that they continue to comply with enterprise business policies and current employee responsibilities

- Status reporting facilities provide information about the current state of identity management data, for example, which users have which roles, which roles are unused, and which users have been given delegated administrative tasks.
- Audit policies define what is audited, and pre-configured audit policies and reports help to jump-start regulatory compliance efforts.

DirX Audit, in turn, provides so-called "detective controls": it provides the features to discover and analyze compliance gaps or high-risk users for follow-up remediation in DirX Identity or DirX Access.

The DirX suite provides the authentication and authorization functionality necessary for the real-time enforcement of the security policies in the enterprise and the identity auditing capabilities required for monitoring and enforcing regulatory compliance.

2. DirX Audit Overview

DirX Audit provides for centralized storage, analysis, correlation and review of identity-related audit trails and historical identity data in a package that is extensible, platform-independent and built on a variety of industry standards.

2.1. DirX Audit Key Features

DirX Audit provides the functional building blocks for a centralized, secure identity audit solution, as shown in the following figure.

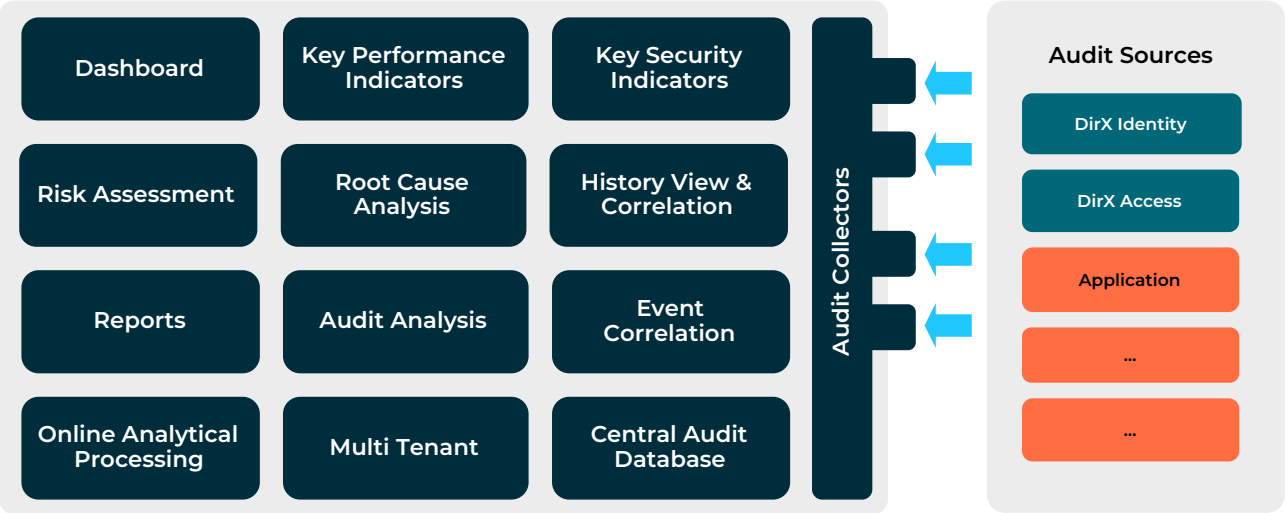

Figure 4. Key Features of DirX Audit

Key features include:

- Convenient correlation of events and activities from different IAM sources in a single Web-based user interface with Dashboard, Audit analysis and History views for different levels of analysis.
- Risk assessment for identities based on a configurable set of risk factors produced in DirX Identity.
- Standard identity audit KPIs that provide statistical information about audit events and historical identity data over a period of time, structured into online analytical processing (OLAP) tables for fast, interactive analysis and insight into IAM operations.
- Dashboard view for analysis of KPI data, with drill-down to more detailed event or history entry information as necessary.
- Audit analysis of audit events retrieved from the central database according to a given search filter and summarized for ease of use, providing auditors and security compliance officers with the answers to the "when, where, who, what and why" of user access and entitlements.
- History view for tracking changes to DirX Identity entries and entry-related data over time, comparing their state at different points in time and checking the state of related entries.

- Reports view for configuring and scheduling the generation and e-mailing of reports for Dashboard, Audit analysis and History view analyses.
- Configurable report templates for Dashboard charts, audit events and history entries for exporting selected audit and historical data to files according to ad hoc filters.
- Automated consolidation of identity-related audit trails with transformation to a standard format and business language, giving DirX Audit users a unified presentation and analysis of audit events from a variety of sources.
- Authentication and authorization against any Lightweight Directory Access Protocol (LDAP) directory.
- Persistent storage of audit trails in both their original and normalized format in a central database.
- Persistent storage of historical identity data in a central database.
- Support for multiple tenants, where each tenant typically represents a DirX Identity domain or a DirX Access installation. All of the tenant-specific data are completely separated from the data of other tenants; in particular, the events and history entries are stored in separate databases.
- Limited access to a tenant's events and history entries for "restricted auditors" (fine-grained access control).

2.2. DirX Audit Components

DirX Audit components provide the basic machinery for analyzing, correlating and storing audit data. These components include:

- DirX Audit Server, a central server that hosts several types of services:
  - Collectors, which collect the audit trails generated from different audit trail producers, transform into normalized format and store them in the DirX Audit Database.
  - Data enrichment services, which translate the audit trails to business-friendly format and attach tags to the audit trails that can be used for KPIs.
  - History Synchronization jobs, which regularly export snapshots of important DirX Identity entries together with time validity and then import them into the central DirX Audit History Database.
  - Post-processing jobs, which aggregate the data from the OLTP tables and their tags into OLAP (KPI) tables. They build the basis for charts and reports.
  - Jobs for running scheduled reports.
- DirX Audit Database, which provides central, secure, persistent storage for audit trails from different audit trail producers, derived OLAP data and DirX Identity history entries.
- DirX Audit Message Broker, which receives audit trails from their producers and forwards them to the Java Message Service (JMS) collectors.
- DirX Audit Manager, a Web-based user interface to the DirX Audit Database for audit administrators, auditors and security and compliance officers.

- Command-line archive tools, which allow audit administrators to archive and restore audit trails in the DirX Audit Database and maintain DirX Audit Database data.

The following figure illustrates these components.

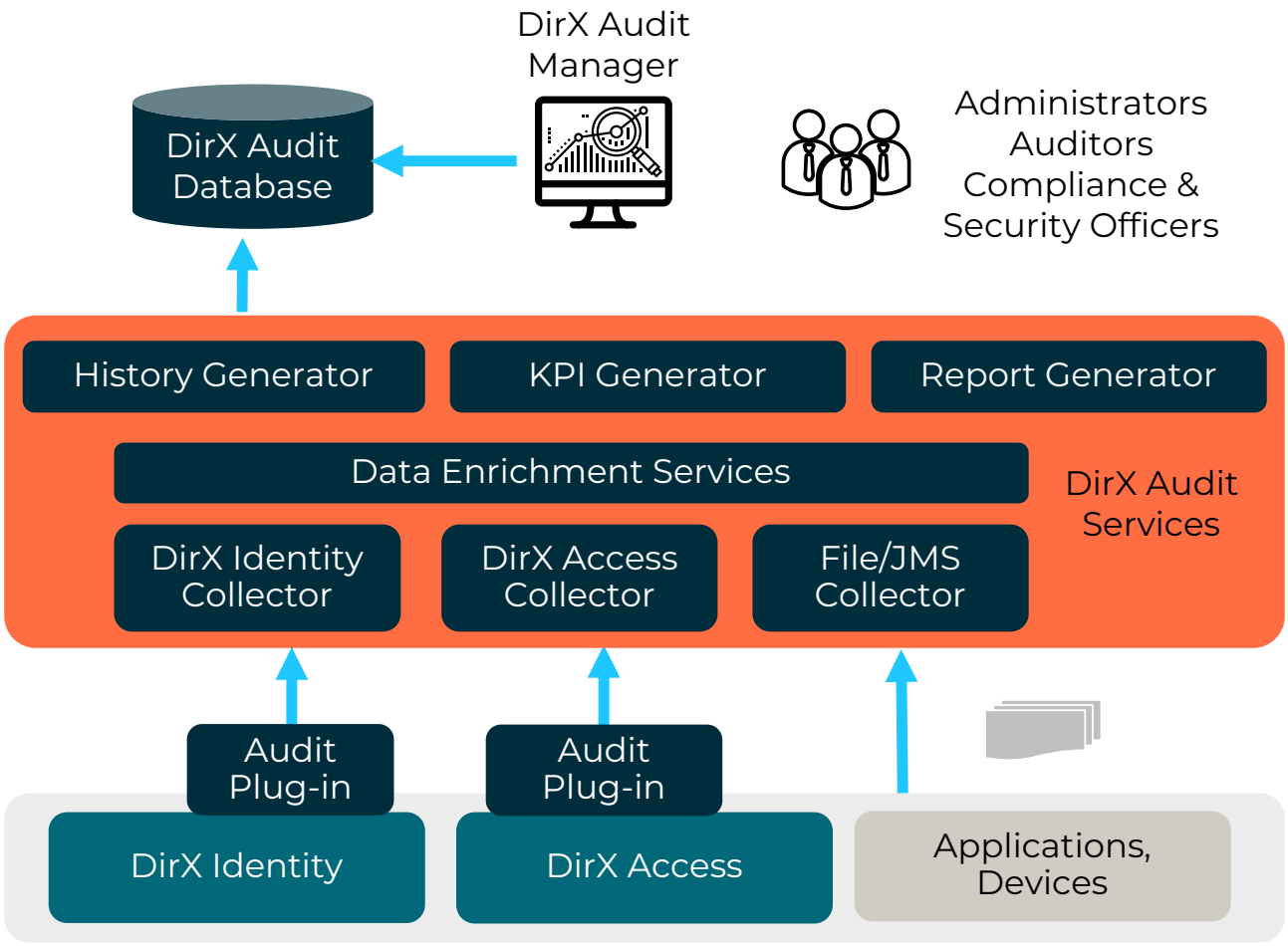

Figure 5. Key Components of DirX Audit

2.2.1. DirX Audit Trail Producers

Both DirX and third-party components can produce audit trails for consumption by DirX Audit:

- Plug-ins in the DirX suite produce audit trails and then pass them to a JMS message queue or an LDAP server or write them to files.
- Third-party applications can provide audit trails that conform to an XML schema defined by DirX Audit and either store them in files or send them to a JMS message queue. These applications are responsible for transforming their native format to DirX Audit's generic XML format.

2.2.2. DirX Audit Server

DirX Audit Server hosts a number of components and services: audit trail collectors and transformers and services for enriching audit messages and history entries and for calculating aggregated data as a basis for charts. These components and services store all their data in the DirX Audit Database.

Collectors retrieve the audit trails from their respective sources and then pass them to services in the DirX Audit Server for transformation, enrichment and storage. DirX Audit collectors can be distinguished according to their technology and the format of the audit trails they are able to consume. They can retrieve audit trails from JMS queues in the DirX Audit Message Broker, from files or from an LDAP directory server.

The collectors forward their audit trails to **transformers**, which convert the audit trail producer's native format (if necessary) to the generic format used by DirX Audit. A transformer is available for audit trails produced by DirX Identity. If the audit trail is already in the DirX Audit native format, no transformation is necessary.

The transformers forward the transformed audit trails to the persistence service, which stores them in the DirX Audit Database.

The **data enrichment services**:

- Generate a business-friendly summary from each raw audit message. These summaries are displayed in the DirX Audit Manager's Audit analysis and in event reports.
- Extract tags from each audit event and history entry and then store them in specific tag tables in the DirX Audit Database. A **tag** labels the data in some way; for example, whether the event was about a password change and whether it was assisted or self-service, or whether the event was about accepting or rejecting an approval. A tag can also, for example, identify the department to which an acting user or an affected user belongs. Tags serve as an additional basis for producing aggregated OLAP (KPI) data; for example, how many assisted password changes or failed logins occur per day or month, or how many orphaned accounts or imported memberships exist at the end of the day or month.

The DirX Audit Server also controls several scheduled jobs:

- The **Scheduled reports** job produces scheduled reports that an auditor has created in DirX Audit Manager.
- The **Context records calculation** finds and links all the events that belong to the same operation's **context**. All (DirX Identity) events in a context were caused by the same root event. For example, a role assignment causes the creation of an account-group membership in the DirX Identity domain and the synchronization to the target system.
- The **History DB update** creates and stores derived attributes that allow for creating and generating richer reports easier and faster. For the most part, these attributes refer to request workflows; for example, whether they were escalated or rejected.

- The **Fact population** (KPI generator) creates and populates the OLAP **fact tables**. These tables are the basis for the graphical charts presented in the DirX Audit Manager's Dashboard view. **Dimension tables** define attributes of the KPIs, while fact tables contain the aggregated statistical information for a set of dimensions (slices). The KPI generator creates and populates the dimension and fact tables based on a customizable configuration that describes a filter for the audit events or history entries to be aggregated in a fact table, the dimensions and the requested facts.
- The **Purge** jobs regularly remove history entries data, audit messages data or original audit messages data that is no more required in the DirX Audit Database.
- The **History Synchronization** jobs create snapshots of DirX Identity domain entries by importing them regularly into the DirX Audit History Database together with their time validity. Entries are processed during the import. The LDAP History Synchronization jobs also synchronize the LDAP schema to the DirX Audit History Database.

2.2.3. DirX Audit Database

The DirX Audit Database is a relational database that works with popular relational database servers such as Microsoft SQL Server and Oracle Database.

The DirX Audit Database provides persistent storage for original and transformed audit trails along with their summary, the history entries imported from DirX Identity, the OLAP tables and the configuration for dashboards, event filters and reports. Audit, history and configuration data are logically partitioned and can be stored in separate databases if necessary.

To maximize the availability of aggregated audit data, DirX Audit supports different lifetimes for audit messages, audit events and OLAP fact tables: fact tables and their associated dimension tables have the longest lifetime, while the complete audit message with all the details has the shortest. As a result, you can delete the details of audit messages and the original messages after a few months, but you can still view the charts on the aggregated data and drill down to the audit event summaries. If disk space subsequently becomes an issue, you can delete the event summaries and still be able to view the charts on the aggregated data.

DirX Audit provides command-line tools that help administrators manage the content of the DirX Audit Database according to audit trail lifetime. For example, audit messages older than six months are automatically exported and/or deleted. All of these messages (or a subset) can be imported back into the DirX Audit Events Database (Data) later on if necessary.

2.2.4. DirX Audit Manager

DirX Audit Manager provides a single, central Web-based interface that offers different views of the audit trails and historical identity data stored in the DirX Audit Database.

The Dashboard view presents identity audit data that the DirX Audit Server has aggregated according to the various identity audit KPIs in graphical charts. DirX Audit provides a standard set of KPIs modeled as OLAP tables to allow for fast display of important aggregated data. Using the Dashboard, auditors can perform analysis, especially time-based trend analysis of selected KPI data - for example, the total number of users created from day to day over a given period of time - and then drill down to details about audit events as necessary.

Audit analysis works directly with **audit events** stored in the DirX Audit Database rather than with aggregated, OLAP-structured KPI data. The Audit analysis view displays page-through tables of audit events retrieved from the DirX Audit Database according to a given search filter. The difference between an audit message and an audit event is as follows: an **audit message** includes the operation, the "where from", "who" and "what" information extracted from the message and the original message in the native format as obtained from the audit producer (for example, DirX Identity). An audit event extends an audit message with one or more informational summaries of the operation recorded by the message and the objects on which it operated. For example, an audit message could cover a couple of group membership changes of one group or one account or it could be associated with a self-registration request workflow that includes the creation of a user along with several role assignments. In these cases, each account-group membership and each role assignment are associated with an extra audit event. As a result, you can have several audit events attached to the same audit message. The operation of an audit event normally contains higher-level, business-friendly information, for example: add assignment, accept add assignment, set password. Additional fields of the event show the object type (user, role, user to role, account to group) and detail information specific to the operation and the object type. For example, for a role assignment, the details contain the user name, the role name, start and end date of the role assignment as well as role parameters and the name of the approval workflow or the name of the approve activity. For a new account-group membership, it contains the names of the account, the group and the target system.

The History view allows an auditor to examine the status (snapshots) of identities and identity-related data at points in time in the past. The auditor can query for entries with their names and for a desired date. Alternatively, the auditor can select a "who" or "what" in the Audit analysis and then request its display in the History view. The History view then displays the entry’s attributes and relationships. In particular, it shows users with their privilege assignments, their accounts, and their risk score. By following the reference links, an auditor can view related entries - for example, the details of an associated role or account. The integrated timeline allows an auditor to compare the state of a selected entry at different points in time. Another tab shows - for a selected time interval - the related audit events on the actions the selected user has performed or the changes that have been applied to the selected entry. The auditor can also ask why the user has a selected privilege assignment. DirX Audit Manager then searches for and shows the root event for this assignment - regardless of whether it has been assigned manually, automatically or by inheritance.

The Reports view allows auditors to set up scheduled reports that can then be sent automatically via e-mail to selected recipients at regular intervals. The auditor defines one or more reports of several types - for example, Dashboard chart, Audit analysis audit events list, snapshot of history entries - associates them with a schedule and enters the mail recipients and text. The DirX Audit Server then manages the regular production of these reports and their delivery to the intended recipients.

Ad hoc reports can be created from all the DirX Audit Manager views based on the current query results and on pre-configured report templates. Reports can be saved to the file system for further distribution and processing. Supported output formats include HTML and PDF. Reports can also be generated in the background to avoid user idle time.

With its intuitive user interface and its access to normalized, centralized audit and history data, DirX Audit Manager simplifies and expedites the laborious, expensive and time-consuming process of sifting through obscurely formatted audit trails generated by many different applications.

Access to DirX Audit Manager is only allowed for auditors. They must be known in LDAP directories and members of auditor groups. DirX Audit distinguishes between audit administrators, normal and restricted auditors. Restricted auditors can only run and schedule reports tagged as restricted.

2.3. Multi-tenancy

One DirX Audit installation can serve multiple tenants. The tenant-specific data - audit events, history entries, and configuration - are completely separated; DirX Audit requires a different database for each tenant. These databases can even be hosted by different database servers. The multi-tenant approach allows access control to be managed using the standard database administration tools.

One DirX Audit Manager application can serve many different tenants, but the auditors of one tenant cannot view the data of another tenant. Auditors of different tenants can reside in the same or in different LDAP servers. They need to use a tenant-specific URL to authenticate.

A separate instance of DirX Audit Server is used for each tenant.

2.4. Customizing and Extending DirX Audit

DirX Audit provides several features for customizing and extension:

- You can connect the audit data from any application to DirX Audit by transforming the native audit trail format to DirX Audit’s generic XML format and using the DirX Audit generic file or JMS collector to collect the audit trails.
- You can customize the Dashboard layout and select KPI data from existing OLAP fact tables and then control how it displays this data.
- You can add your own OLAP tables for use in the Dashboard view.

- You can add your own OLAP dimension producer components and then use these dimensions in the OLAP tables.
- You can create your own database tables and then integrate them into OLAP data production and into reports.
- You can customize the default reports or create your own reports.

2.5. Standards Support in DirX Audit

DirX Audit components support several standards for connectivity, authentication and authorization, storage and data formatting:

- The DirX Audit Server is implemented as a Spring Boot application.
- The DirX Audit Server uses Java Message Service (JMS) for the collection of audit trails.
- The DirX Audit Server uses the public domain components of the Java Management Extension (JMX) technology for DirX Audit Server monitoring.
- The DirX Audit Database uses Structured Query Language (SQL) for internal audit data management and retrieval.
- The DirX Audit Manager uses Lightweight Directory Access Protocol (LDAP) for user authentication.
- The DirX Audit Server uses Lightweight Directory Access Protocol (LDAP) for the collection of audit trails.
- The DirX Audit Server uses Lightweight Directory Access Protocol (LDAP) for the collection of history entries.
- The DirX Audit Manager uses Extensible Access Control Markup Language (XACML) for user authorization to the DirX Audit Database.
- The DirX Audit Manager is a Java Server Faces (JSF)-based Web application.

3. Glossary

This glossary defines terms and concepts that relate to DirX Audit and identity and access management. Additional information about identity and access management terminology can be found in the glossary of the *DirX Identity Introduction* and in the *DirX Access Glossary*.

A

access certification: The process of periodically checking user-privilege assignments to ensure that these assignments continue to comply with business policies.

access management: The part of an IAM system that performs real-time enforcement of the security policies established for each user of the enterprise IT infrastructure. Access management processes include authentication, authorization, and audit.

administration: The process of managing digital identities and access across the heterogeneous IT environment through a combination of user roles and business rules.

audit: See identity audit.

audit event: Information about a discrete operation within a logical sequence of IAM operations recorded in an audit message. An audit event contains a reference to the audit message and an additional information summary. Several audit events may be associated with an audit message. For example, an audit message on a group modification may cover several account-group membership changes. Each account-group membership change makes up an audit event, with summary information on the account, the group and the specific operation and the additional information from the audit message that is common to all associated account-group events. See also audit message.

audit message: A message in an audit trail that DirX Audit has extracted, transformed into DirX Audit data format and stored in the DirX Audit Database. The data in the audit message includes the original message in the format of the audit producer plus the "where from", "who", and "what" and information and a message identification. See also audit event.

audit trail: A chronological sequence of audit messages, where each message contains evidence that directly pertains to and results from the execution of an IAM transaction. See also audit message, audit event.

authentication: The process of identifying users and validating their identity.

authorization: The real-time enforcement of user access requests to the enterprise resources. Authorization ensures that users can only access the IT systems in the enterprise and their corresponding resources according to their access rights.

C

collation: The rules for character representation and the comparison and sorting of data in a relational database system (SQL server, Oracle Database). When you select a collation for your server, database, column, or expression, you assign certain characteristics to the data, and these characteristics affect the results of different operations in the database.

compliance (regulatory compliance): The clear and demonstrable observation of legal or other regulations.

compound risk score: The calculated compound score for the user. All the user's standard scores are used to compute the compound score.

D

digital identity: See identity.

DirX Audit Audit analysis: The DirX Audit Manager view that displays a table of audit events retrieved from the DirX Audit Database according to a given search filter. Each row in the table displays one audit event and its associated information.

DirX Audit collector: The DirX Audit component that imports audit trails generated by a particular type of audit trail producer.

DirX Audit Dashboard: The DirX Audit Manager view that presents identity audit key performance indicators (KPIs) in a graphical format; typically, as charts.

DirX Audit Database: The DirX Audit component that provides consolidated, persistent storage for audit messages, audit events, history entries, OLAP data structures (dimensions and facts) and meta data, and configuration information.

DirX Audit History: The DirX Audit Manager view that displays the state of an entry in a DirX Identity domain at a given point in the past. DirX Audit History Synchronization jobs regularly import identity and identity-related state changes to history entries in the DirX Audit History Database, where they are available for analysis. The History view allows auditors to compare identity state at different points in time, check the state of related entries, observe all entry-related events in a given time interval and investigate causal events for a specific assignment.

DirX Audit Manager: The DirX Audit component that provides a graphical user interface for the correlation, analysis and review of audit and historical identity data. The DirX Audit Manager provides Dashboard, Audit analysis, History and Reports views for different levels of analysis.

DirX Audit Reports: The DirX Audit Manager view that allows auditors to set up scheduled configurable reports that can be sent via e-mail to selected recipients at regular intervals by the DirX Audit Server.

DirX Audit Server: The DirX Audit component that hosts DirX Audit collectors, performs normalization, transformation and storage on collected audit messages, creates OLAP data structures (dimension and fact tables), generates audit event information and runs jobs for creating and delivering reports.

E

entitlement: The access right of a user in a target system; for example, a group assignment. Identity governance functions discover entitlements in target systems and then use them to create aggregated privileges like permissions and business roles. Privilege resolution determines, as a consequence of role assignment and user context information like attributes and role parameters, the set of entitlements that need to be provisioned. See the DirX Identity Introduction for more information.

H

history entry: The state of an entry in a DirX Identity domain at a specific point in the past.

I

identity: A single unique view of a user to be provisioned in the enterprise IT infrastructure that is aggregated from multiple authoritative sources of user data in the enterprise IT infrastructure by the IAM system's metadirectory services. Also called "digital identity".

identity and access management (IAM): An integrated solution for user and access management across the heterogeneous systems that constitute the IT infrastructure of an enterprise.

identity audit: The process of producing, collecting, cleansing and correlating data about IAM administration, authentication and authorization events and then transforming this data into actionable intelligence with respect to compliance regulations, business security policies and corporate risk management objectives. Identity audit provides the means to analyze and report on IAM functioning and deliver the information necessary to support IAM governance of users and their entitlements.

identity federation: An application of authentication that permits an enterprise to share trusted identities with autonomous organizations outside of the enterprise, like trading partners or suppliers. Also called federated identity and federation.

identity management: The part of an IAM system that ensures a consolidated, enterprise-wide view and way to manage user access to resources in the enterprise IT infrastructure, aligning enterprise business interests with lower-level IT operations for user management and provisioning. Identity governance functions provide a high-level, transparent way to define, create, manage, assign, review and remove users and their entitlements according to business security objectives and compliance requirements. Identity provisioning functions dynamically and automatically realize the results of identity governance operations into the necessary entitlements in the enterprise IT infrastructure. Identity management processes include user self-service and delegated administration, password management, user management, role, policy and business object management, request workflow, access certification, real-time provisioning and reconciliation and metadirectory.

K

key performance indicator (KPI): In industry jargon, a type of measure of performance (see http://en.wikipedia.org/wiki/Performance_indicator for a definition). In DirX Audit, a KPI is associated with statistical information on a subset of audit events.

key risk indicator (KRI): In industry jargon, a type of measure to indicate how risky an action or a subject is.

M

multi-tenancy: The ability to support, configure and run multiple tenants. See also tenant.

O

online analytical processing (OLAP) schema: A method of modeling data according to a "cube" type of data structure that allows for fast, interactive manipulation and analysis of the data (called "facts") from multiple perspectives, called "dimensions". See http://en.wikipedia.org/wiki/Online_analytical_processing for more information.

online transactional processing (OLTP) schema: A method of modeling data to achieve efficient transactions such as insertions and deletions. See http://en.wikipedia.org/wiki/Online_transaction_processing for more information.

R

report: In casual use, a report may refer, for example, to a report template in the form of a JRXML document or the output file generated when a report is run and scheduled or exported. Here we understand a report more specifically as a JasperReport. A JasperReport is a combination of a report template and data that produces a complex document for viewing, printing, or archiving information. It is defined by a report creator and generated when the report is run and shown in the Web application, scheduled or exported. At the heart of a JasperReport is the report template. It is a JRXML document, an XML standard and defines precisely all the structure and configuration of a report. The template references information about the data source that supplies data for the report and additional resources, such as images, fonts, and resource bundles for localization of text. The collection of all the resources that are referenced in a JasperReport is sometimes called a report unit. End users usually see and interact with a JasperReport as a single resource, but report creators must define all of the components in the report unit.

report set: One or more report files to be sent, the schedule for when to send them, and who is to receive them. Each report file has a defined format and contains one or more individual reports.

risk level: The overall risk level for the user. Possible values are Low (1), Medium (2) or High (3).

risk score: The standard score for the risk factor. This value is a normalized score for the factor at the user.

S

segregation of duties (SoD): The process of placing constraints on role assignment to enforce "conflict of interest policies", for example, a user with the role "accounts payable" cannot be assigned the role "accounts receivable". Also called separation of duties.

single risk factor: A single element that contributes to the risk assessment of a user. Examples of single risk factors include the total number of group memberships, the total number of SoD violations, the total number of imported memberships, the total number of imported accounts, and the total number of privileged accounts. See also compound risk score.

SoD policy: A policy that specifies the roles that cannot be assigned to a user at the same time. See also segregation of duties (SoD).

T

tenant: A DirX Identity domain or a DirX Access installation. All of the data maintained in DirX Audit that are specific to a particular tenant are kept separate from other tenants, including audit events, history data, fact tables, reports, chart components and the configuration data such as database connection settings, authentication and authorization settings, audit sources, server task configurations, and Message Broker users and queues. See also the definition of a domain in the DirX Identity Introduction and https://en.wikipedia.org/wiki/Multitenancy.

W

Web access management: Access management for users and applications that attempt to access IT resources via a Web browser and/or Web protocols. See also access management.

DirX Product Suite

The DirX product suite provides the basis for fully integrated identity and access management; it includes the following products, which can be ordered separately.

DirX Identity

DirX Identity provides a comprehensive, process-driven, customizable, cloud-enabled, scalable, and highly available identity management solution for businesses and organizations. It provides overarching, risk-based identity and access governance functionality seamlessly integrated with automated provisioning. Functionality includes lifecycle management for users and roles, cross-platform and rule-based real-time provisioning, web-based self-service functions for users, delegated administration, request workflows, access certification, password management, metadirectory as well as auditing and reporting functionality.

DirX Directory

DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable, highly scalable, and secure LDAP and X.500 Directory Server and LDAP Proxy with very high linear scalability. DirX Directory can serve as an identity store for employees, customers, partners, subscribers, and other IoT entities. It can also serve as a provisioning, access management and metadirectory repository, to provide a single point of access to the information within disparate and heterogeneous directories available in an enterprise network or cloud environment for user management and provisioning.

DirX Access

DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy- and risk-based authentication, authorization based on XACML and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication including FIDO, identity federation based on SAML, OAuth and OpenID Connect, just-in-time provisioning, entitlement management and policy enforcement for applications and services in the cloud or on-premises.

DirX Audit

DirX Audit provides auditors, security compliance officers and audit administrators with analytical insight and transparency for identity and access. Based on historical identity data and recorded events from the identity and access management processes, DirX Audit allows answering the “what, when, where, who and why” questions of user access and entitlements. DirX Audit features historical views and reports on identity data, a graphical dashboard with drill-down into individual events, an analysis view for filtering, evaluating, correlating, and reviewing of identity-related events and job management for report generation.

For more information: support.dirx.solutions/about

EVIDEN

Legal remarks

On the account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this document are available through the Eviden sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available locally. The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases. Eviden reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Eviden sales representative for the most current information. Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.