Evidian

DirX Audit V7.0

Effiziente Compliance-Unterstützung

Analyse und Transparenz für Identity und Access

Die Herausforderung

Kostendruck und steigende Sicherheitsanforderungen lassen Unternehmen und Organisationen über neue Möglichkeiten nachdenken, wie sie ihre Geschäftsprozesse weiter optimieren können. Dies gilt insbesondere für die Einhaltung von Compliance-Vorschriften, wie sie beispielsweise in der EU-Datenschutzgrundverordnung hinsichtlich der Verarbeitung persönlicher Daten oder im Sarbanes Oxley Act für die Verlässlichkeit veröffentlichter Finanzdaten von Unternehmen geregelt sind. Eine Maßnahme, diese Vorhaben effizient zu unterstützen, ist die Einführung eines Identity und Access Management Systems (IAM) in Verbindung mit entsprechender Analytics und Intelligence Unterstützung.

Die große Anzahl von Regulierungen stellt jedoch eine Herausforderung dar:

- Heute existieren viele unterschiedliche Vorschriften und ständig kommen neue hinzu, was eine laufende Überarbeitung der IAM-Steuerungsmechanismen erfordert.
- Die Vorgaben für das, was zu auditieren ist, hängen sowohl von der speziellen Vorschrift als auch vom jeweiligen Geschäftsmodell des Unternehmens sowie von der Anwendung ab, die die Audit-Daten erzeugt. Dies erschwert es, konsistente und durchgängige Audit-Leitlinien zu etablieren.
- Unterschiedliche Vorschriften erfordern unterschiedliche Methoden der Analyse und Berichterstattung.

Zum Nachweis von Rechenschaftspflichten und zur Berichterstattung über die Ergebnisse von IAM-Aktivitäten müssen Audit-Daten erzeugt werden. Wie von den maßgeblichen Vorschriften gefordert, dient dies zur Darstellung, wie die Steuerung der Geschäftsprozesse hinsichtlich der Benutzerzugriffe und -berechtigungen erfolgt. In regelmäßigen Abständen oder bei Bedarf müssen Reports zum aktuellen Status und zur Historie von Informationen in den IAM-Datenhaltungen erzeugt werden, zum Beispiel für die Identity-Datenhaltung in einer Identity Management Komponente.

Die Audit-Daten sowie die historischen Daten, die von den IAM-Komponenten erzeugt werden, helfen dabei, die Fragen zu beantworten, die von Auditoren zum Nachweis der Einhaltung der Compliance gestellt werden. Bisher müssen für Fragen der Art "Wer hat im letzten Monat auf Finanzdaten zugegriffen?", "Wer hat den Benutzern dafür Zugriffsrechte gegeben?" und "Wer hat diese Rechte genehmigt?" Audit- und historische Daten aus mehreren Anwendungen ausgewertet werden. Unterschiedliche Audit-Formate, verschiedene Benutzer-Identitäten derselben Person sowie parallele Zeitstränge in den einzelnen Anwendungen erschweren diese Auswertungen erheblich und machen sie kostenintensiv.

Unsere Lösung

DirX Audit bietet Auditoren, Sicherheitsbeauftragten und Audit-Administratoren analytischen Einblick und Transparenz in Identity und Access Management Prozesse. DirX Audit ergänzt die IAM-Kernfunktionen für Administration, Authentifizierung und Autorisierung um Funktionen zur Analyse und Berichterstattung über IAM-Operationen und stellt die Informationen bereit, die zur Unterstützung von IAM Governance, des Risikomanagements und zum Nachweis der Compliance benötigt werden.

Basierend auf historischen Identitätsdaten und aufgezeichneten Aktivitäten aus den Identity und Access Management Prozessen ermöglicht DirX Audit die Beantwortung der "Was, Wann, Wo, Wer und Warum"-Fragen bei Benutzerzugriffen und -berechtigungen. DirX Audit bietet historische Ansichten und Reports für Identitätsdaten, ein grafisches Dashboard mit Drill-Down zu einzelnen Ereignissen, einen Monitor zum Filtern, Analysieren, Korrelieren und Überprüfen von Identitäts-bezogenen Aktivitäten und die Verwaltung von Jobs für die Reporterstellung. Mit seinen Analyse-Funktionen unterstützt DirX Audit Unternehmen und Organisationen bei der nachhaltigen Einhaltung von Compliance-Anforderungen und stellt Business Intelligence für die Identity und Access Management Prozesse bereit.

In Abbildung 1 sind die Funktionsblöcke dargestellt, die DirX Audit für eine zentrale und sichere Analytics und Intelligence Lösung zur Verfügung stellt.

Zu den wesentlichen Funktionen und Eigenschaften von DirX Audit gehören:

- Die einfache Korrelation von Events und Aktivitäten aus verschiedenen IAM-Quellen über eine Web-basierte Benutzerschnittstelle mit Dashboard, Event Monitor und historischen Ansichten zur Unterstützung für unterschiedliche Analyse-Level
- Risikoanalyse für Identitäten basierend auf konfigurierbaren Risikofaktoren
- Standard Key Performance Indikatoren (KPI), die statistische Informationen zu Audit-Events und historischen Identitätsdaten über einen auswählbaren Zeitraum zur Verfügung stellen. Zur schnellen, interaktiven Analyse und Einsicht in IAM-Operationen werden KPIs in Online Analytical Processing (OLAP) Tabellen erfasst
- Ein Dashboard mit KPI- und Trendanalyse-Diagrammen mit Drill-Down zu detaillierten Informationen zu Events oder zu historischen Identitäten
- Ein Event Monitor für Audit-Events, die gemäß dem eingestellten Suchfilter und zur einfacheren Nutzung zusammengefasst dargestellt sind. Die Audit-Events liefern Auditoren und Sicherheitsbeauftragten die Antworten zu den „Was, Wann, Wo, Wer und Warum" Fragen für Benutzerzugriffe und -berechtigungen
- Historische Ansichten zum Nachverfolgen von Änderungen von Identitäten und Identitäts-bezogenen Daten über die Zeit, mit der Möglichkeit, den Zustand von Identitäten in der Vergangenheit anzusehen und Vergleiche zwischen Zeitpunkten durchzuführen
- Report-Verwaltung zum Einrichten von Zeitplänen für Jobs zur Erstellung und für den Email-Versand von Reports für die Analysen aus Dashboard, Event Monitor und historischen Ansichten
- Konfigurierbare Vorlagen für Reports für Dashboard Diagramme, Audit Events und historische Einträge zum Exportieren ausgewählter Audit- und historischer Daten in Dateien
- Konfigurierbare Vorlagen für das Dashboard-Layout und für Diagramme zur Analyse von Audit-KPI-Daten nach verschiedenen Kriterien
- Verständliche Aufbereitung von Identitäts-bezogenen Audit-Daten, was DirX Audit Benutzern eine einheitliche Darstellung und Analyse von Audit-Events aus verschiedenen Quellen liefert
- Authentifizierung gegen einen Lightweight Directory Access Protocol (LDAP) Directory Server; Autorisierung basierend auf Gruppenmitgliedschaften im LDAP Directory Server
- Persistente Speicherung der Audit-Daten in einer zentralen Datenbank sowohl in ihrem originalen als auch in einem normalisierten Format

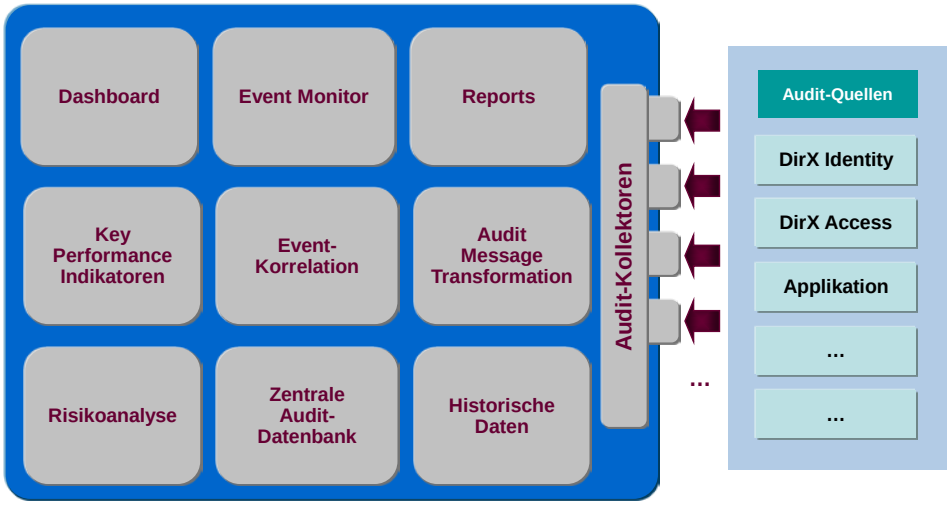

Abb. 1: DirX Audit Funktionalität

- Persistente Speicherung von historischen Identitätsdaten in einer zentralen Datenbank
- Integration mit Archivierungslösungen mittels Purge- und Restore-Funktionen
- Unterstützung mehrerer Mandanten (DirX Identity Domänen)
- Erweiterbar, um Audit-Events anderer Anwendungen zu sammeln
- Unterstützung von Organisations- oder Abteilungsauditoren, die nur die Events ihrer Organisation sehen.

Dashboard

Das Dashboard im DirX Audit Manager präsentiert Event-Daten und historische Daten, die der DirX Audit Server entsprechend der unterschiedlichen Identity Audit KPIs aufbereitet, in grafischen Diagrammen. DirX Audit stellt einen Standardsatz von KPIs zur Verfügung, die als OLAP-Tabellen modelliert sind, um eine schnelle Anzeige von wichtigen Audit-Daten zu ermöglichen. Durch die Nutzung des Dashboards können Auditoren Analysen durchführen, speziell zeitbasierte Trendanalysen von ausgewählten KPI-Daten, zum Beispiel die Gesamtanzahl von angelegten Benutzern pro Tag über einen gewählten Zeitraum, und dann, wenn benötigt, weitere Detailinformationen anzeigen. Die Diagramme können als Balken-, Kreis-, Linien-, Punkt- oder Area-Diagramme dargestellt werden, wie in Abbildung 2 als Beispiel zu sehen ist.

Das Dashboard stellt KPI-Diagramme zur Verfügung für

- Events zu Accounts, Account-Gruppen-Mitgliedschaften, Benutzer, Benutzer-Rollen-Zuordnungen, Passwortänderungen, Passwortabfragen, Genehmigungen, Authentifizierungen, Autorisierungen, etc. mit allen, erfolgreichen und fehlgeschlagenen Operationen, durchgeführten und abgewiesenen Genehmigungen,
- Historische Daten zu Identitäten mit der Gesamtanzahl der Einträge,

die kategorisiert werden können über: Zeit (Jahr, Monat, Tag), Operationen, Applikationen, Objekttypen, Auditkomponenten, Organisationseinheiten des Benutzers, automatische oder manuelle Zuweisungen, etc.

Andere Beispiele für Analysen, die von Auditoren durchgeführt werden können, sind

- Wie viele Account-Änderungen wurden in einem Zielsystem durchgeführt?
- Wie viele Account-Gruppen-Mitgliedschaften wurden von einem Zielsystem importiert?
- Wie ist der Trend bei der Kategorisierung der Benutzer in Risikoklassen?
- Wie viele Rollenzuweisungen wurden genehmigt?
- Wie viele Passwörter wurden geändert? Wie viele der Passwortänderungen sind fehlgeschlagen?
- Wie viele Identitäten wurden verwaltet?
- Wie viele Ausnahmen zu Funktionstrennungen wurden ermittelt?
- Wie viele Accounts sind verwaist?
- Wie viele Zertifizierungskampagnen wurden durchgeführt?
- Wie viele (Risiko-)Benutzer wurden letztes Jahr nicht zertifiziert?

Ein Audit-Administrator kann einen Satz von öffentlichen Diagramm-Konfigurationen bereitstellen, der für alle Auditoren direkt verfügbar ist. Die Auditoren selbst können ihre privaten Diagramm- und Dashboard-Layouts definieren und diese in lokalen Dateien speichern und wieder daraus importieren.

Event Monitor

Der Event Monitor im DirX Audit Manager ermöglicht Auditoren die Suche und das Abrufen von Audit-Events aus der zentralen DirX Audit Datenbank gemäß einem eingestellten Suchfilter.

Der Event Monitor arbeitet direkt mit den Audit Events, die in der DirX Audit Datenbank gespeichert sind, anstatt mit den aggregierten, gemäß OLAP strukturierten KPI-Daten. Ein Audit Event erweitert die Information in der ursprünglichen, detaillierten Audit-Nachricht mit einer oder mehreren Zusammenfassungen von Informationen zu Operationen, die mit der Nachricht aufgezeichnet wurden, und zu betroffenen

Objekten. Diese Zusammenfassungen können Auditoren dabei unterstützen, selbst komplexe Operationen wie die Genehmigung einer Benutzer-Rollen-Zuweisung mit Änderung des Ende-Datums und einem neuen Rollenparameter leicht zu verstehen.

Auditoren können den Suchfilter für folgende Parameter konfigurieren:

- Wann, Von und Bis: Relativer oder absoluter Zeitraum, zum Beispiel letzter Monat, letztes Jahr, etc. oder vom Anwender einstellbares Start- und Ende-Datum
- Quelle: Diejenige Komponente, die den Audit-Event erzeugt hat
- Wer: Der Benutzer, der den Audit-Event initiiert hat
- Was: Das Objekt, das mit dem Event verknüpft ist, zum Beispiel der Name des Benutzer, des Accounts, der Rolle, etc.
- Event-Typ: Der Operationstyp des Events, d.h. wie die Operation initiiert wurde, zum Beispiel manuell, termingesteuert oder auf Anforderung
- Operation: Die Operation des Events, zum Beispiel Passwort setzen, Zuweisung hinzufügen, Objektänderung anfordern, Objekt hinzufügen oder löschen, Login, Logout, etc.
- Objekt-Typ: Der Objekt-Typ, der mit dem Event verknüpft ist, zum Beispiel Benutzer, Account, Account-Gruppenmitgliedschaft
- Detail: Spezielle Details einer Operation auf einem Objekttyp, zum Beispiel ein spezieller Account oder ein spezielles Zielsystem bei einer Suche nach Update-Operationen für Accounts

Das Feld Detail des Suchfilters ermöglicht das Filtern von Audit-Events nach speziellen Details wie zum Beispiel:

- Rollenzuweisung der Rolle „Projektmanager“ an den Benutzer Max Mustermann
- Anforderung einer Rollenzuweisung der Rolle “Erste Klasse” mit dem Startdatum 7. Juni 2018 nach dem 4-Augen-Prinzip
- Genehmigung der vorhergehenden Anforderung
- Account-Gruppen-Zuweisung des Benutzers Max Mustermann zur Gruppe “Erste Klasse” im Zielsystem „Extranet Portal“

Der Event Monitor zeigt eine Liste von Audit-Events als Ergebnis der mit dem eingestellten Suchfilter durchgeführten Suche an. Zu jedem der Events können zusätzliche detailliertere Informationen durch einfachen Mausklick auf ein Icon angezeigt werden.

Speziell kann eine Kette von Events, die zum selben Kontext gehören, angezeigt werden. Zum Beispiel die Events, die zu einer neuen Gruppenmitgliedschaft geführt haben oder die Webzugriffe eines Benutzers innerhalb derselben DirX Access Session. Die Ergebnisliste kann als Report in eine Datei exportiert werden. Aus der Detail-Ansicht kann man direkt in die historische Ansicht wechseln.

Abb. 2: DirX Audit Dashboard - Beispiel

Historische Ansicht

Die historische Ansicht im DirX Audit Manager ermöglicht es dem Auditor, den Zustand von Identitäten und Identitäts-bezogenen Daten zu Zeitpunkten in der Vergangenheit zu untersuchen. Der Auditor kann Einträge über ihren Namen und das gewünschte Datum suchen. Alternativ kann der Auditor ein Wer oder Was im Event Monitor auswählen und den gefundenen Eintrag in der historischen Ansicht anzeigen lassen. Daraufhin wird auf der Zeitachse der Status des Eintrags vor und nach dem Zeitpunkt des Events angezeigt.

Für einen gewählten Eintrag zeigt die historische Ansicht eine grafische Darstellung der Zeitachse mit denjenigen Zeitpunkten, an denen der Eintrag erzeugt, geändert oder gelöscht wurde. Durch entsprechendes Hinein- oder Hinauszoomen kann der Auditor den Fokus auf ein für ihn interessantes Zeitintervall richten.

Zusätzlich werden Details der Attribute und der Beziehungen des Eintrags für ausgewählte Zeitpunkte angezeigt. Für Identitäten umfasst dies die Zuordnungen von Rollen, Rollenparametern und Accounts sowie die Risikoklassifizierung. Für Rollen umfasst dies alle Identitäten, denen die Rolle zugeordnet ist. Durch Verfolgen von Referenzlinks kann der Auditor zugehörige Einträge anzeigen, zum Beispiel die Details einer zugehörigen Rolle oder eines zugehörigen Accounts.

Für einen ausgewählten Eintrag können die zugehörigen Events angezeigt werden, die den Eintrag geändert haben oder die der Benutzer durchgeführt hat. Zudem unterstützt DirX Audit die Ursachenanalyse für die Zuordnung von Privilegien wie beispielsweise in Abbildung 3 dargestellt.

Report-Verwaltung

In der Report-Verwaltung vom DirX Audit Manager können Auditoren Zeitpläne für Jobs zum Erzeugen und Versenden von Reports einrichten. Ein Report-Job versendet eine Email mit einer oder mehreren Report-Dateien, wobei jede Datei einen oder mehrere Reports enthalten kann. Ein einzelner Report kann ein Dashboard-Diagramm, eine Liste von Audit-Events oder eine Momentaufnahme von historischen Einträgen sein. Die Zeitpunkte zur Erzeugung von Reports sind typischerweise periodisch wiederkehrend, zum Beispiel einmal pro Monat. Ein Auditor kann jedoch auch einen einmaligen Versand festlegen, entweder für eine Uhrzeit an einem bestimmten Datum oder sobald wie möglich. Für die Email legt der Auditor die Email-Empfänger und den Text fest. Der DirX Audit Server sorgt für die termingerechte Erzeugung und den Versand der Reports an die spezifizierten Empfänger.

Reports können Parameter enthalten, mit denen ihr Geltungsbereich festgelegt werden kann. Da sie typischerweise periodisch erzeugt werden, muss die Zeitperiode festgelegt werden, zum Beispiel der vorige Monat.

Andere Parameter legen basierend auf Attributen wie Namen der Einträge, Risikolevel, Namen der Zielsysteme, Organisationseinheiten oder bestimmter Privilegien die Auswahl der Events oder Einträge fest.

Einige Reports enthalten einen Platzhalter in ihren Filterkriterien, so dass ihr Ergebnis vom Autor des Reports abhängt. Zum Beispiel enthält der Report dann nur die Events der Organisationseinheit des Autors.

DirX Audit stellt eine Reihe von Standard-Reports zur Verfügung, zum Beispiel

- Zugriffsanforderungen gefiltert nach Benutzer, Antragsteller oder Privileg
- Änderungen bei Accounts und Gruppen in bestimmten Zielsystemen
- Logins, speziell fehlgeschlagene Login-Versuche
- Überblick über verwaiste, importierte oder deaktivierte Accounts für alle oder für ausgewählte Zielsysteme
- Überblick über importierte Gruppenmitgliedschaften
- Liste der Benutzer in den verschiedenen Risikoklassen
- Überblick über bestimmte Benutzer inklusive ihrer Accounts oder Rollen und Gruppen
- Ungenutzte Privilegien, d.h. Privilegien, die

weder einem Benutzer noch einer Rolle zugewiesen sind
- Benutzer mit bestimmten Rollen- oder Gruppenzugehörigkeiten
- Genehmigungs-Workflows und Kampagnen zur Berechtigungsprüfung, sowohl noch laufende als auch bereits beendete
- Details von laufenden oder im letzten Monat durchgeführten Zertifizierungskampagnen
- Liste von Benutzern, die im vergangenen Jahr nicht zertifiziert wurden.

Reports zu Audit-Events können Informationen zur anfordernden Person, zu der den Event verursachenden Regel und zu den Genehmigern enthalten.

Durch kundenspezifische Anpassungen können Administratoren basierend auf den mitgelieferten Beispielen eigene Reports erstellen oder vorhandene Reports anpassen.

Basierend auf aktuellen Ergebnissen von Abfragen und mittels vordefinierter Report-Vorlagen können Reports auch aus anderen Ansichten des DirX Audit Managers erzeugt werden. Als Ausgabeformate werden HTML und PDF unterstützt. Die Reports können im Dateisystem zur weiteren Verteilung und Verarbeitung abgespeichert werden.

Event-Korrelation

In der Event Monitor Sicht unterstützen Kontext-Abfragen beim Auffinden zugehöriger Audit-Events für einen bereits selektierten speziellen Event. Ein Beispiel ist der Login für den Zugriff auf eine Ressource. Ein weiteres Beispiel ist die Rollenzuweisung, die das Hinzufügen eines Benutzers in eine bestimmte Gruppe ausgelöst hat, die wiederum den Zugriff auf eine bestimmte Ressource in einem angeschlossenen System ermöglicht.

Risikoanalyse

Um die Benutzer in Risikoklassen einzuordnen, wie zum Beispiel risikoreiche und risikoarme Benutzer, werden regelmäßig Risikofaktoren berechnet und gemäß einer kundenspezifisch anpassbaren Konfiguration gespeichert. Beispiele für Risikofaktoren sind: Verletzungen von Funktionstrennungen, importierte Accounts und Gruppenmitgliedschaften oder die Gesamtanzahl von Gruppenmitgliedschaften eines Benutzers. Diese Werte und ihre gewichteten Summen werden sowohl in der History Sicht von DirX Audit Manager als auch in entsprechenden Diagrammen und Reports angezeigt. Compliance Manager können dann risikoreiche Benutzer genauer untersuchen und Maßnahmen zur Reduktion von Risiken einleiten.

Sicherheit

Um den Zugriff auf DirX Audit abzusichern, verlangt DirX Audit, dass sich seine Benutzer authentifizieren und dass ihr Zugriff auf DirX Audit und seine Daten autorisiert wird.

Authentifizierung und Autorisierung

DirX Audit Benutzer können gegen beliebige

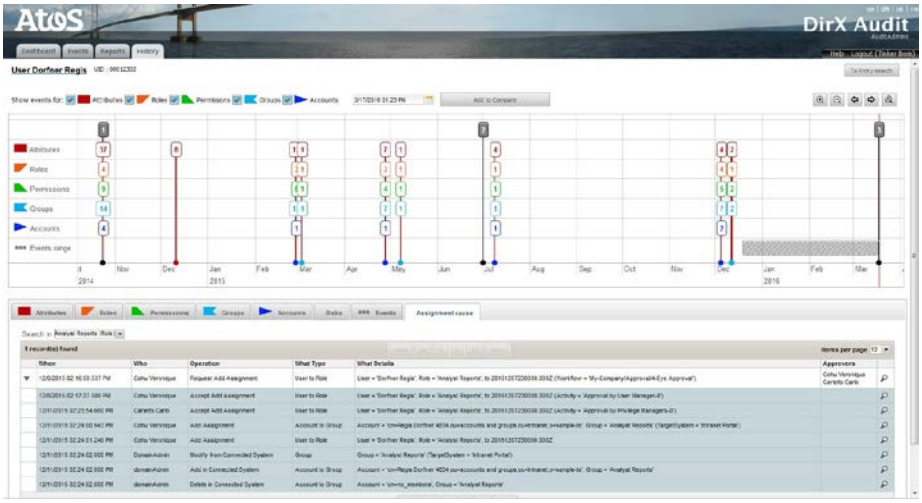

Abb. 3: DirX Audit Historische Ansicht Beispiel - Ursachenanalyse für Rollenzuweisung

LDAP Directories (Lightweight Directory Access Protocol) authentifiziert werden.

Zur Autorisierung des Zugriffs werden in DirX Audit folgende Benutzergruppen unterschieden:

- Audit-Administratoren – diese können alle öffentlichen Diagramm-Komponenten (Dashboard Sicht) und alle öffentlichen Filter (Event Monitor) sehen und verwalten.
- Auditoren – diese können die öffentlichen Diagramme und die öffentlichen Event-Filter sehen und sie können ihr privates Dashboard-Layout und ihre privaten Diagramme und Event-Filter sehen und verwalten.
- Auditoren mit eingeschränkten Rechten: diese können nur die mit dem Tag RESTRICTED versehenen Reports sehen jedoch nicht das Dashboard, den Event Monitor und die historische Ansicht. Eingeschränkte Reports enthalten Platzhalter als Filtereinschränkungen, so dass die Reportausgabe nur die Benutzer der Organisationseinheit des Reportautors enthält.

Anmerkung: Die Mitgliedschaft eines Benutzers in konfigurierbaren Gruppen in dem LDAP-Directory, das zur Authentifizierung genutzt wird, legt die Auditor-Rolle des Benutzers innerhalb DirX Audit fest. In DirX Identity beispielsweise sind dies zwei vordefinierte Gruppen, Auditors und AuditAdmins, die durch Rollen gesteuert werden.

Autorisierung für Audit-Daten

DirX Audit unterstützt eine feingranulare Zugriffskontrolle für die Audit-Datensätze. Es können Access Policies definiert werden, die den Zugriff auf die Audit-Daten basierend auf deren Inhalt einschränken. Zum Beispiel, wenn Auditoren nur die zu ihrer Organisationseinheit gehörenden Datensätze sehen dürfen, d.h. wenn Objekte ihrer Organisationseinheit geändert wurden oder wenn Mitarbeiter ihrer Organisationseinheit Aktionen durchgeführt haben.

Die Policies für die Zugriffskontrolle werden als XACML-Policies (eXtensible Access Control Markup Language) in Form von Obligations für die SQL-Abfragen implementiert. DirX Audit implementiert seinen eigenen Policy Enforcement Point (PEP) mit Policies, die in lokalen Dateien gespeichert sind, oder kann optional DirX Access für die zentrale Datenhaltung der Policies und als zentrales System zur Ermittlung von Zugriffs-Entscheidungen (Policy Decision Point, PDP) nutzen. Die Obligations können von den Audit-Administratoren mittels DirX Access Manager konfiguriert werden. Normalerweise werden die Policies auf LDAP-Gruppen angewendet, sie können jedoch auch auf den Attributen des LDAP-Eintrags des Auditors basieren.

Transformation von Audit-Daten

Audit-Daten können aus unterschiedlichen Quellen mit jeweils eigenem Originalformat kommen. Transformationskomponenten sorgen für die Umwandlung vom Originalformat in das Standardformat von DirX Audit.

Das Konzept der Anreicherung erlaubt es, Audit-Daten zu ergänzen. Dies wird speziell dazu genutzt, um eine informative Zusammenfassung für jeden Audit-Datensatz zu erzeugen und abzulegen.

Zusätzlich erzeugen spezielle Komponenten eine Reihe von Tags für jeden importierten Datensatz, die die Basis zur Befüllung der Fakten und Dimensionen der OLAP-Würfel bilden.

Kundenspezifische Transformations- und Anreicherungsfunktionen können auf Auditdaten von Applikationen angewendet werden, die nicht standardmäßig von DirX Audit unterstützt werden. Zusätzlich können Kunden eigene Tags für die von DirX Identity und DirX Access erzeugten Audit-Events erstellen.

Persistente Audit Datenbank

Audit-Daten werden sowohl in ihrem Originalformat als auch im normalisierten Format sicher in einer zentralen Datenbank gespeichert.

Audit-Datenquellen wie DirX Identity können ihre Audit-Daten mit einer System-spezifischen, digitalen Signatur gesichert zur Verfügung stellen, um sie gegen Manipulationen zu schützen. Wenn sie in der DirX Audit Datenbank gespeichert sind, können sie nicht geändert werden, ohne dass es mittels der Signatur

erkannt werden kann. Ebenso können Audit-Daten-Lieferanten wie DirX Identity Client-signierte Audit-Daten zur Verfügung stellen, um Nachweise für Transaktionen bereitzustellen, die mittels IAM-Policies als risikoreich eingestuft wurden.

Zum Archivieren werden Purge und Restore der Datenbank oder von Teilen der Datenbank im XML-Format unterstützt.

Zur Reduzierung der Größe der archivierten Daten wird ein Komprimierungsverfahren eingesetzt. Zusätzlich können Backup und Restore mittels der Datenbank-eigenen Tools durchgeführt werden.

Zur Verlängerung der Verfügbarkeit der Daten unterstützen die DirX Audit Archivierungstools unterschiedliche Lebenszyklen für die Audit-Daten und für die OLAP-Fakten-Tabellen. Die Fakten-Tabellen haben die längste Lebenszeit, während die vollständigen Audit-Daten mit all ihren Einzelheiten die kürzeste Lebenszeit haben. Der Administrator kann die meisten Details der Audit-Daten und die originalen Datensätze nach einigen Monaten exportieren und löschen, jedoch die wichtigsten Basisdaten und die Zusammenfassungen behalten. Dies ermöglicht den Auditoren, weiterhin die Diagramme für die aggregierten Daten und die zugehörigen informativen Zusammenfassungen zu sehen, um die durchgeführten Operationen zu verstehen. Wenn der Administrator später auch die Zusammenfassungen der Audit-Daten zum Beispiel wegen fehlendem Plattenspeicherplatz löscht, existieren immer noch die OLAP-Würfel, die es ermöglichen, Diagramme zu den aggregierten Daten zu sehen.

Mandantenfähigkeit

Eine DirX Audit Installation kann mehrere Mandanten unterstützen, zum Beispiel mehrere DirX Identity Domänen.

Die DirX Identity Domänen können im gleichen oder in unterschiedlichen LDAP-Servern liegen. Die Audit-Events und historischen Momentaufnahmen jedes Mandanten werden in separaten Audit-Datenbanken gespeichert. So kann der Zugriff auf Daten anderer Mandanten einfach verhindert werden.

Jeder Mandant kann, basierend auf gemeinsamen Templates, seine eigenen Reports und Diagramme konfigurieren und erzeugen.

Administration

Audit-Administratoren und Auditoren sind typischerweise für die Verwaltung von Abfragen, Reports und zur Verwaltung der Zugriffskontrolle zuständig. Die Systemverwaltung umfasst darüber hinaus folgende Aufgaben:

- die Verwaltung des DirX Audit Managers
- die Verwaltung des DirX Audit Message Brokers
- die Verwaltung des DirX Audit Servers
- die Verwaltung der Datenbanken
- die Verwaltung der Audit-Plugins in den Produkten, die die Audit-Daten erzeugen (DirX Identity, DirX Access)
- die Verwaltung der Mandanten und ihrer jeweiligen Datenbanken und Message Queues.

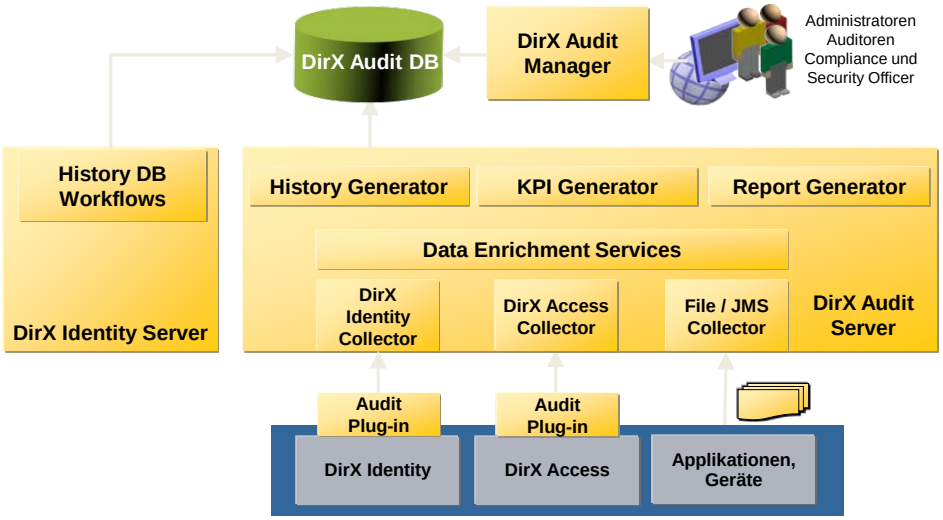

Abb. 4: DirX Audit Architektur

Kundenspezifische Anpassung und Erweiterbarkeit

DirX Audit ist so ausgelegt, dass es in Bezug auf die Abfragen, die Reports und die Anzeige der Objekte an der Benutzerschnittstelle kundenspezifisch angepasst und erweitert werden kann. Dazu gehören:

- die Anbindung der Audit-Daten beliebiger Applikationen durch Umwandlung des ursprünglichen Audit-Datenformats in das generische Format von DirX Audit und das Importieren der Audit-Daten mit der generischen DirX Audit Message Queue (JMS) oder dem File-Kollektor von DirX Audit
- die kundenspezifische Anpassung des Dashboard-Layouts und Auswahl von KPI-Daten von existierenden OLAP-Fakten-Tabellen sowie das Festlegen, wie die Daten angezeigt werden sollen
- das Hinzufügen eigener OLAP-Tabellen zur Nutzung in der Dashboard-Sicht
- das Hinzufügen eigener Erzeugungskomponenten für OLAP-Dimensionen mit anschließender Nutzung dieser Dimensionen in den OLAP-Tabellen
- die kundenspezifische Anpassung der Standard-Reports zur Nutzung im Event Monitor
- das Erzeugen kundenspezifischer Reports mittels SQL und Platzhaltern
- das Hinzufügen spezifischer Attributwerte zu vordefinierten Abfragen
- die Definition kundenspezifischer Abfragen
- Kundenspezifische Anpassung des Tabellenlayouts von Abfrageergebnissen wie zum Beispiel die Sichtbarkeit von Spalten
- das Erzeugen kundenspezifischer Seiten: sie basieren auf der Technologie Java Server Faces (JSF) und enthalten ausgewählte User Interface-Komponenten des DirX Audit Managers. Die Komponenten, ihre Zusammenstellung und ihr Layout liegen vollständig in der Kontrolle des Kunden.
- das Hinzufügen zusätzlicher Sprachen zum DirX Audit Manager; der DirX Audit Manager wird standardmäßig mit zwei Sprachen geliefert: Englisch und Deutsch
- das Einrichten von Single Sign-On Http Header Injection; dies kann genutzt werden, um den DirX Audit Manager in bestehende Web Access Management oder Web Single Sign-On Lösungen zu integrieren.

DirX Audit Architektur

Die DirX Audit Komponenten stellen die Basis-Umgebung zur Analyse, Korrelation und Speicherung von Audit-Daten zur Verfügung.

Zu diesen Komponenten gehören:

- der DirX Audit Server, ein zentraler Server, der Audit-Daten sammelt, transformiert und anreichert und sie in die DirX Audit Datenbank speichert
- die DirX Audit Datenbank, die die zentrale, sichere und persistente Speicherung der Audit-Daten unterschiedlicher Quellen, der historischen Einträge aus DirX Identity sowie der daraus abgeleiteten OLAP-Daten zur Verfügung stellt
- der DirX Audit Manager, eine Web-basierte Benutzerschnittstelle zur DirX Audit Datenbank für Auditoren, Sicherheits- und Compliance-Beauftragte, Audit-Administratoren und Benutzer
- Kommandozeilen-Archivierungstools, die den Audit-Administratoren das Archivieren in und Wiederherstellen aus der DirX Audit Datenbank sowie die Pflege der Audit-Daten in der DirX Audit Datenbank ermöglichen
- History Datenbank Synchronisations-Workflows, die in DirX Identity eingerichtet werden, um DirX Identity Einträge periodisch in die zentrale DirX Audit Datenbank zu synchronisieren.

In Abbildung 4 wird die DirX Audit Architektur mit ihren Integrationspunkten in verschiedene Anwendungen aus einer high-level Sicht dargestellt.

DirX Audit Server

Der DirX Audit Server ist die zentrale Drehscheibe für das Sammeln und Analysieren von Identitäts-bezogenen Daten:

- Kollektoren sammeln die Audit-Daten von ihren jeweiligen Quellen und leiten diese zur Transformation, Anreicherung und Speicherung an die Services im DirX Audit Server weiter. Kollektoren können je nach Typ Audit-Daten aus unterschiedlichen Quellen erhalten: aus JMS Message Queues im DirX Audit Message Broker, aus Dateien oder aus einem LDAP Directory Server.
  Die generischen JMS- und File-Kollektoren von DirX Audit können dazu genutzt werden, beliebige Anwendungen mit DirX Audit zu verbinden.
  In diesem Fall muss das Audit-Datenformat mit dem von DirX Audit genutzten generischen Datenformat kompatibel sein und eine kundenspezifische Komponente muss eingesetzt werden, um die Daten um eine Business-orientierte Zusammenfassung zu erweitern.
- Data Enrichment Services wandeln die Audit-Daten in ein Business-orientiertes Format um und versehen die Audit-Daten mit Tags, die für die KPIs genutzt werden können.
- Jobs zur Nachbearbeitung aggregieren Daten der OLAP-Tabellen sowie die Tags in OLAP-Würfel. Diese bilden die Grundlage für Diagramme und Reports.
- Der History Generator pflegt die Beziehungen zwischen historischen Einträgen und ergänzt die Einträge um abgeleitete Attribute, um reichhaltigere und schnellere Reports und KPIs zu ermöglichen.
- Der KPI Generator erzeugt und füllt die OLAP-Würfel (Fakten-Tabellen zusammen mit ihren Dimensionen) basierend auf einer kundenspezifisch anpassbaren Konfiguration, die einen Filter für diejenigen Audit-Daten und historischen Einträge definiert, die in einer Fakten-Tabelle, den Dimensionen und den angeforderten Fakten aggregiert werden sollen. Diese Tabellen sind die Grundlage für die Diagramme, die im Dashboard vom DirX Audit Manager angezeigt werden.
- Der Report Generator erzeugt zu den festgelegten Zeitpunkten auf Basis der Report-Definitionen die Reports.

DirX Audit Datenbank

Die DirX Audit Datenhaltung ist eine relationale Datenbank wie Microsoft SQL Server oder Oracle Datenbank. Die Datenbank wird für die persistente Speicherung von Konfigurations- und Eventdaten sowie von historischen Daten genutzt.

DirX Audit Manager

Der DirX Audit Manager stellt eine zentrale Web-basierte Benutzerschnittstelle mit unterschiedlichen Sichten auf die in der DirX Audit Datenbank gespeicherten Audit- und historischen Identitätsdaten zur Verfügung. Zusätzlich bietet der DirX Audit Manager:

- Einfache Korrelation von Events und Aktivitäten aus verschiedenen IAM-Quellen in einer einzigen Benutzeroberfläche mit Dashboard und Event Monitor Sichten für unterschiedliche Level von Analysen.
- Zeitpunkt-Analysen von historischen Identitäten und Identitätsbezogenen Daten, die von DirX Identity in die DirX Audit Datenbank synchronisiert wurden.
- Einrichten und Festlegen der Zeitpunkte für die automatische Reporterstellung für Analysen von Audit- und historischen Daten.
- Öffentliche und private Analyse-Tools mit unterschiedlichen Stufen für den Zugriff, wie zum Beispiel öffentliche und private Dashboard-Komponenten oder öffentliche und private Event-Filter.
- Vorkonfigurierte Objekte, wie OLAP-Würfel und Dashboard-Komponenten, die helfen, schnell Ergebnisse bei den durchzuführenden Audit- und Compliance Aufgaben zu erhalten, und die an spezifische kundenspezifische Anforderungen angepasst werden können.

Mit seiner intuitiven Benutzerschnittstelle und dem Zugriff auf normalisierte, zentrale Audit-Daten, erleichtert und beschleunigt der DirX Audit Manager den aufwendigen und teuren Prozess des Durchsuchens unterschiedlich formatierter Audit-Daten, die von verschiedenen Anwendungen erzeugt werden, und ermöglicht die Untersuchung der Zustände von Identitäten für zurückliegende Zeitpunkte.

Der DirX Audit Manager ermöglicht die öffentliche und private Verwaltung des Dashboards und der Abfragen und stellt eine Reihe von vorkonfigurierten OLAP-Würfeln, Dashboard-Diagrammen, Abfragen, Reports und Statistiken zum einfachen Einstieg in Audit- und Compliance-Aufgaben zur Verfügung. Vorkonfigurierte Reports, Statistiken und Diagramme können kundenspezifisch an spezielle Anforderungen angepasst werden oder mit zusätzlichen Tools wie Jaspersoft Studio von Grund auf neu erzeugt werden.

Workflows für DirX Identity History-Daten

Die Workflows für die History Datenbank werden beim Java-basierten Identity Server von DirX Identity eingerichtet. Jeder Workflow synchronisiert einen relevanten Typ von Einträgen – zum Beispiel Benutzer, Rollen, Accounts, Gruppen oder Organisationseinheiten – und erzeugt Momentaufnahmen von DirX Identity Einträgen des jeweiligen Typs durch regelmäßiges Importieren der Einträge in die DirX Audit History Datenbank. Jobs zur Nachverarbeitung im DirX Audit Server ergänzen diese History-Einträge speziell mit Risikostufen und erzeugen OLAP-Würfel, die die Grundlage für History Reports und Diagramme und die historische Ansicht im DirX Audit Manager sind.

Die Workflows für die History Datenbank können auch im Delta-Modus laufen: dann exportieren sie nur diejenigen Einträge, die sich seit dem letzten Lauf geändert haben. Diese Funktion setzt mindestens DirX Identity V8.3 voraus.

Ausfallsicherheit und Hochverfügbarkeit

Die Ausfallsicherheit und Hochverfügbarkeit der Datenhaltung beruht auf den Funktionen und Eigenschaften der eingesetzten Datenbank.

Zusätzlich ist DirX Audit in der Lage, eine temporär nicht erreichbare Datenbank durch automatisches Recovery wieder verfügbar zu machen.

Unterstützte Standards

Die DirX Audit Komponenten unterstützen folgende Standards für Konnektivität, Authentifizierung und Autorisierung, Speicherung bzw. Datenformate:

- Der DirX Audit Server ist als Sammlung von OSGi (Open Services Gateway initiative) Services implementiert, die auf dem Apache ServiceMix Enterprise Service Bus (ESB) betrieben wird.
- Der DirX Audit Server unterstützt Java Messaging Service (JMS) für die Sammlung der Audit-Daten.
- Der DirX Audit Server nutzt die Public Domain Komponenten der Java Management Extension (JMX) zur Überwachung des DirX Audit Servers.
- Der DirX Audit Manager nutzt das Lightweight Directory Access Protocol (LDAP) für die Authentifizierung und Autorisierung der Benutzer.
- Der DirX Audit Manager nutzt XACML (eXtensible Access Control Markup Language) Policies für die Zugriffskontrolle zur DirX Audit Datenbank.
- Der DirX Audit Manager ist eine Java Server Faces (JSF)-basierte Web-Applikation.
- Die DirX Audit Datenbank nutzt Structured Query Language (SQL) für die interne Audit-Daten-Verwaltung und die Datensuche.

Weitere DirX Produkte

Die DirX-Produktfamilie bietet die Basis für ein vollständig integriertes Identity- und Access-Management; zur DirX-Produktfamilie gehören neben DirX Audit folgende Produkte, die separat bestellt werden können:

- DirX Directory stellt einen standardkonformen, leistungsstarken, hochverfügbaren, sehr zuverlässigen und sicheren LDAP und X.500 Directory Server mit sehr hoher linearer Skalierbarkeit zur Verfügung. DirX Directory kann als Identity-Datenhaltung für Informationen über Mitarbeiter, Kunden, Geschäftspartner, Abonnenten von Diensten sowie über andere Teilnehmer von eBusiness-Verfahren dienen.
- DirX Identity stellt eine umfassende, prozessgesteuerte, kundenspezifisch anpassbare, Cloud-fähige, skalierbare und hochverfügbare Identity Management Lösung für Unternehmen und Organisationen zur Verfügung. Es stellt übergreifende Identity und Access Governance Funktionalität bereit, die nahtlos mit automatisiertem Provisioning integriert ist. Die Funktionalität umfasst Life-Cycle-Management für Benutzer und Rollen, plattformübergreifendes und regelbasiertes Provisioning in Echtzeit, Web-basierte Self-Service-Funktionen für Benutzer, delegierte Administration, Antrags-Workflows, Berechtigungsprüfung, Passwortmanagement, Metadirectory sowie Audit- und Report-Funktionalität.
- DirX Access ist eine umfassende, Cloud-fähige, skalierbare und hochverfügbare Access Management Lösung, die Policy-basierte Authentifizierung, Autorisierung und Federation für Web-Applikationen und -Services bietet. DirX Access bietet Single Sign-On, vielfältige Authentisierungsmöglichkeiten einschließlich risikobasierter Authentifizierung, Identity Federation basierend auf SAML, OAuth und OpenID Connect, Just-in-Time Provisioning, Entitlement Management und die Durchsetzung von Sicherheits-Policies für Anwendungen und Dienste in der Cloud oder intern im Unternehmen.

Technische Voraussetzungen für DirX Audit V7.0

Hardware

- Intel Server Plattform für Microsoft Windows Server 2012 R2 und 2016, Red Hat Enterprise Linux Server 7, SUSE Linux Enterprise Server 12

Speicherplatzanforderung:
Hauptspeicher: mindestens 8 GB
Plattenspeicher: mindestens 10 GB plus Plattenspeicher für Daten

Software

Der DirX Audit Server als Java-Anwendung wird auf folgenden Plattformen unterstützt:

- Microsoft Windows Server 2012 R2 und 2016 (x86-64)
- Red Hat Enterprise Linux Server 7 (x86-64)
- SUSE Linux Enterprise Server 12 (x86-64)

Für die gewählte Plattform sind die aktuellsten Patches/Service Packs erforderlich.

Unterstützung virtueller Maschinen:

- VMWare ESXi 6.0 in Kombination mit den oben genannten Gast-Betriebssystemen, die für VMWare ESXi 6.0 freigegeben sind

Unterstützte Datenbanken:
DirX Audit unterstützt die folgenden Datenbanken:

- Microsoft SQL Server Enterprise or Standard Edition 2014, 2016 und 2017
- Oracle Database 12c

Unterstützte Browser für den DirX Audit Manager

- Microsoft Internet Explorer 11
- Microsoft Edge
- Firefox 38.0 ESR oder neuer
- Google Chrome

DirX Audit Manager
DirX Audit Manager erfordert die Installation von Apache Tomcat 8 oder 9 mit den aktuellsten Patches/Service Packs.

Optional, DirX Access V8.7 mit Patch MR#2915 für die feingranulare Zugriffskontrolle für Audit-Daten.

DirX Audit Event Kollektoren

- Der Kollektor für DirX Identity unterstützt DirX Identity ab V8.4
- Der Kollektor für DirX Access unterstützt DirX Access V8.4/V8.5/V8.7

Report-Erzeugung:

- Erfordert Jaspersoft Studio 5.6 oder neuer

Benutzeroberfläche

Englisch, Deutsch, Französisch

Dokumentation

- Release Notes (Textfile, Englisch)
- Installation Guide (Manual, Englisch)
- Migration Guide (Manual, Englisch)
- Introduction (Manual, Englisch)
- Tutorial (Manual, Englisch)
- Administration Guide (Manual, Englisch)
- User Interface Guide (Manual, Englisch)
- Customization Guide (Manual, Englisch)
- History Database Synchronization Workflows (Manual, Englisch)

Manuale werden im PDF und Web Help Format geliefert; Installation Guide und Migration Guide nur im PDF-Format.

More information:
www.evidian.com

Alle Warenzeichen sind Eigentum ihrer jeweiligen Rechteinhaber. Atos, das Atos logo, Atos Codex, Atos Consulting, Atos Worldgrid, Bull, Canopy, equensWorldline, Unify, Worldline und Zero Email sind eingetragene Warenzeichen der Atos Gruppe. Atos behält sich das Recht vor, dieses Dokument jederzeit ohne Vorankündigung zu ändern. Einige in diesem Dokument beschriebenen Angebote oder Teile von Angeboten können lokal nicht verfügbar sein. Bitte kontaktieren Sie Ihre Atos Stelle für Informationen über das Angebot in Ihrem Land. Dieses Dokument stellt keine vertragliche Verpflichtung dar. Oktober 2018. © 2018 Atos