DirX Access V8.7

Vertrauensvolle Zusammen-arbeit

Access Management und Identity Federation für die vernetzte Welt

Alles und jeder ist online, und das Absichern des Zugriffes auf Anwendungen oder Geräte, die intern und extern oder in der Cloud bereitgestellt werden, war niemals zuvor wichtiger als heutzutage.

Unternehmen und öffentliche Verwaltungen forcieren die Entwicklung von Online-Partnerschaften, um schnell mögliche Einnahmequellen erschließen zu können, sie lagern Dienste, die nicht zum Kerngeschäft gehören, aus und bieten ihren Nutzern vielfältigste Dienste an. Um die Effizienz zu erhöhen und um auf entsprechende Benutzeranforderungen zu reagieren, werden mehr und mehr sicherheitskritische Daten und Anwendungen online zur Verfügung gestellt - zur gemeinsamen Nutzung von Informationen und für den Self-Service von Verbrauchern, mobilen Mitarbeitern, Geschäftspartnern und Lieferanten.

Die Nutzung der Cloud steigt rapide, da sich gezeigt hat, dass dies für viele Unternehmen und Organisationen durch die kostengünstigere und flexible Art, Anwendungen und Dienste zu nutzen, zu großen Einspareffekten führt.

Mittlerweile erwarten die Nutzer von Online-Diensten, dass diese immer verfügbar sind, dass sie im Sinne eines One-Stop-Shopping Erlebnisses durch ein einziges Login zugreifbar sind und dass sie das gleiche Look and Feel haben, gleich welche Art von Business-Transaktion sie durchführen.

Mit den jüngsten Nachrichten von massiven Sicherheitslücken in Online-Datenbanken und der Verbreitung von Phishing, Spoofing und anderen betrügerischen Online-Aktivitäten, beginnen die Nutzer sich Sorgen darüber zu machen, dass sie zu viel von ihren kritischen Identity-Informationen bei zu vielen Web-Seiten preisgeben. Während Nutzer mehrere unterschiedliche digitale Identitäten haben wollen, um ihre Privatsphäre zu schützen, kann das Erzeugen und Pflegen einer eins-zu-eins Identity-Zuordnung zu jedem einzelnen Online-Service-Provider eine lästige Aufgabe werden, die zu unsicheren Zugangsberechtigungsdaten führt.

Der Aufbau eines agilen, virtuellen Unternehmens, das interne Anwendungen oder private oder öffentliche Cloud- oder Software-as-a-Service Angebote nutzt, führt zu einigen Herausforderungen, um in diesem Umfeld durchgehende Sicherheit zu gewährleisten. Mit Aufkommen von Cloud, Mobile und Social Computing ist die Notwendigkeit für eine verstärkte Zugriffskontrolle stark gestiegen und es muss sichergestellt werden, dass die Zugriffskontrolle mit den Authentisierungs- und Autorisierungsrichtlinien der Organisation übereinstimmt. Geschäftspartner müssen ihre Identitätsdaten austauschen oder integrieren, aber dieses muss geschehen, ohne ihre IT-Administration zu überlasten oder versehentlich Sicherheitslücken zu erzeugen.

Um die Benutzerzufriedenheit zu maximieren, muss eine sichere, nahtlose Transaktion zwischen Diensten unterschiedlicher Sites in unterschiedlichen Security-Domänen zur Verfügung gestellt werden, und diese Transaktionen müssen komplett von Anfang bis zum Ende auditierbar sein, um die Einhaltung von behördlichen und internen Vorschriften nachzuweisen. Um die Benutzerfreundlichkeit weiter zu verbessern, werden Single Sign-On Verfahren gefordert, um das Login sowohl für interne als auch für externe Cloud-Anwendungen und -Dienste zu vereinfachen,

Um schnellen Zugriff auf Cloud-Anwendungen für neue Benutzer bereitzustellen, müssen Verfahren zur Verfügung stehen, um die neuen Benutzer schnell im System einrichten zu können, so dass die aufwendige, manuelle Administration dieser Benutzer in jedem einzelnen SaaS-Directory vermieden werden kann. Die Partner müssen zudem Sicherheitsmodelle für Online-Transaktionen der Nutzerdaten berücksichtigen, die die Sammlung und Kontrolle der Identitätsinformationen weg von den Online Service Providern in die Hände ihrer Benutzer verlagern und die Verwaltung dieser Informationen in die Hände von Identity Providern legen.

Bull
atos technologies

Benutzer von Web- oder Cloud-Services geben oftmals persönliche und vertrauliche Informationen preis. Dies ist mit einem wachsenden Risiko für Sicherheits- und Datenschutzprobleme verbunden. Sobald ein Benutzer einmal derartige Informationen herausgegeben hat, hat er nur noch begrenzte Möglichkeiten, den Zugriff auf diese Informationen zu steuern. Um dieses Problem zu entschärfen, gibt es einen offensichtlichen Bedarf für neue Ansätze und Methoden, die es dem Benutzer ermöglichen, den Zugriff auf seine Web-Ressourcen und –Daten zu kontrollieren.

Die neue Generation von Access Management mit DirX Access

All diese Herausforderungen treiben den Aufbau und den Einsatz neuer Sicherheitsmodelle für das Access Management voran. Identity Federation und sichere Web Services liefern zusammen mit Authentifizierung, Autorisierung, Audit und Web Single Sign-On (SSO) die wesentlichen Funktionen, um Web-Ressourcen auf flexible Art und Weise vor unberechtigter Nutzung zu schützen.

DirX Access ist eine umfassende Access Management, Identity Federation und Web Services Security Lösung, die Ressourcen vor unberechtigter Nutzung schützt.

DirX Access:

- sorgt für die konsistente Durchsetzung von geschäftsrelevanten Sicherheits-Richtlinien durch externe, zentrale und Policy-basierte Authentifizierungs- und Autorisierungs-Services
- verbessert die Benutzerschnittstelle durch lokales und föderiertes Single Sign-On (SSO)
- sichert eGovernment- und eBusiness-Initiativen und sorgt für nahtlose Integration mit Geschäftspartnern und Partnerorganisationen mittels Identity Federation
- schützt Web Services und Applikationen mittels Authentifizierungs- und Autorisierungs-Services, sowohl im Unternehmen selbst als auch in der Cloud
- unterstützt vielfältige Autorisierungsszenarien einschließlich Benutzer-kontrolliertem Zugriff (User-Managed Access)
- entkoppelt Sicherheitsfunktionalität wie Authentifizierung und Autorisierung von den Applikationen und ermöglicht so ein konsistentes, feingranulares Entitlement Management über mehrere Applikationen und Services hinweg
- Ermöglicht Unternehmen und Service Providern, Lösungen für starke Authentifizierung einzusetzen, die die Abhängigkeit von Passwörtern reduzieren
- unterstützt die Einhaltung behördlicher und interner Vorschriften mittels Audit-Funktionalität sowohl innerhalb einer Security-Domäne als auch über mehrere Security-Domänen hinweg.

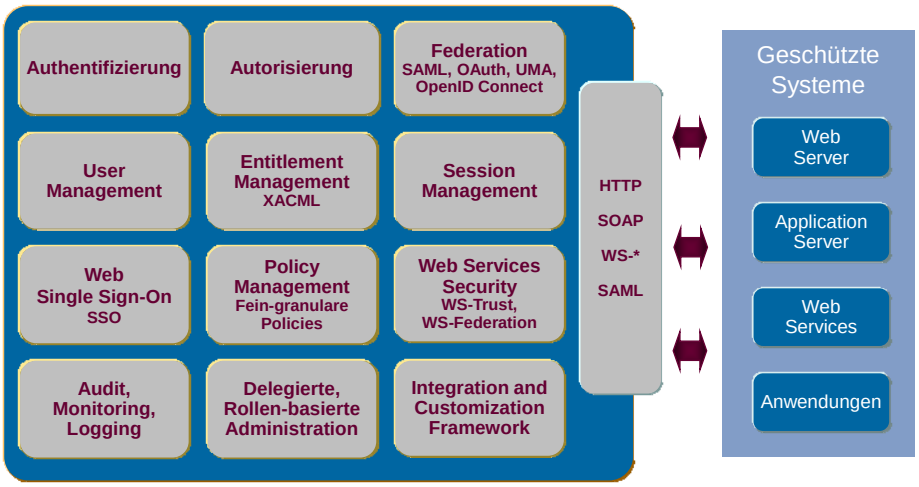

Abb. 1: DirX Access Funktionalität

Authentifizierung, Autorisierung und Audit – Die Kernfunktionalität für Access Management

Authentifizierung ist der Prozess, der die Identität einer Person verifiziert, die Zugriff auf einen Service oder eine Ressource anfordert, während Autorisierung der Prozess ist, der entscheidet, ob ein authentifizierter Benutzer das Recht hat, auf einen gewünschten Service oder eine Ressource zuzugreifen. Authentifizierung beantwortet die Frage „Wer sind Sie?“, während Autorisierung die Frage beantwortet „Was sind Sie berechtigt zu tun?“.

Authentifizierung und Autorisierung setzen die Sicherheitsregeln des Unternehmens oder der Organisation durch, während das Audit automatisch die Transaktionen aufzeichnet und die zugehörigen Daten für die spätere Zusammenfassung in Reports sicher abspeichert, um analytischen Einblick und Transparenz für die Identity und Access Management Prozesse zu bekommen.

Diejenigen Prozesse und Technologien, die genutzt werden, um die Benutzer und ihren Lebenszyklus innerhalb einer Organisation zu verwalten, werden als Identity Management bezeichnet. Diejenigen Prozesse und Technologien, die die Zugriffskontrollregeln für die angeschlossenen Applikationen, Services und Systeme verwalten, zum Einsatz bringen, durchsetzen und auditieren, werden als Autorisierungs- oder Entitlement Management bezeichnet.

Authentifizierung

Mit DirX Access wird Authentifizierung als ein externer, zentraler Service bereitgestellt, der eine Reihe bekannter Authentifizierungsmethoden unterstützt, wie zum Beispiel Passwörter, X.509 Zertifikate, integrierte Windows-Authentifizierung, Smartcards, HTML Forms, One-Time Password (OTP), Biometrie und Callback oder Authentifizierung über einen zweiten Kanal (out-of-band). Administratoren können diejenige Methode zum Einsatz bringen, die am besten die Sicherheitsanforderungen jeder einzelnen Applikation oder Ressource erfüllt, ohne die Applikation ändern zu müssen. Die Entkopplung der Authentifizierung von der Applikation oder Ressource ermöglicht eine einfache Skalierbarkeit des Authentifizierungsservice - Administratoren können neue Authentifizierungsmethoden hinzufügen, ohne Auswirkung auf die Applikationen, die diesen Service nutzen.

Darüber hinaus ermöglichen zentrale Authentifizierungs-Services auch das Single Sign-On (SSO). Dabei geben die Benutzer nur einmal ihre Anmeldedaten (Credentials) ein, und können danach auf alle Applikationen und Ressourcen innerhalb der Sicherheitsdomäne des Unternehmens zugreifen, für die sie autorisiert sind, ohne dass sie nochmals eine Authentifizierung / ein Login durchführen müssen.

Letztendlich ermöglicht der zentrale Authentifizierungs-Service von DirX Access, die Authentifizierungsverwaltung in einer einzigen konfigurierbaren Komponente zu konzentrieren. Da ein externer, zentraler Service die Notwendigkeit für eine Authentifizierung für jede einzelne Applikation eliminiert, müssen die Benutzer sich nicht länger mehrere Login-Credentials merken, und die Administratoren müssen nicht länger redundante Authentifizierungsmechanismen unterstützen.

Die Authentifizierungsservices von DirX Access können in folgende Kategorien unterteilt werden: Initiale Benutzer-Authentifizierung, risikobasierte Authentifizierung, Single Sign-On (SSO) und föderierte Authentifizierung.

Initiale Benutzer-Authentifizierung

Mit initialer Authentifizierung ist das erste Mal gemeint, bei dem ein Benutzer vom System authentifiziert wird. Sie basiert auf der Benutzerkennung, die bei DirX Access bekannt ist und nutzt Standard-basierte Authentifizierungsmechanismen, wie:

- SSL/TLS Client Authentication basierend auf X.509 Zertifikaten inklusive Pfad-Validierung, OCSP- und CRL-Unterstützung
- HTTP Basic Authentifizierung mittels Username/Passwort
- HTML-Formular-basierte Authentifizierung mittels Username/Passwort
- HTML-Formular-basierte Authentifizierung

mit One Time Passwort Algorithmen basierend auf IETF RFC 2289, IETF RFC 4226 (HOTP) und IETF RFC 6238 (TOTP)
- HTTP Authentifizierung durch integrierte Windows-Authentifizierung (IWA) mittels SPNEGO, Kerberos und NTLM
- Microsoft Windows Hello
- FIDO U2F (Universal 2nd Factor)

DirX Access unterstützt Multifaktor-Authentifizierung, indem zwei oder mehrere Authentifizierungsmethoden sequentiell miteinander kombiniert werden können, zum Beispiel Benutzername/Passwort plus zusätzlicher Verifizierung mittels One-Time-Passwort oder Benutzername/Passwort plus einer externen Validierung, etc.

DirX Access kann die Anmeldedaten (Credentials) der Benutzer selbst intern validieren (dies ist die Standardoption) oder die Validierung an einen externen Validierungsservice auslagern. Die externe Validierung ist offen für diverse Algorithmen, eine Schnittstelle für Verifizierungsverfahren anderer Hersteller unterstützt Token-artige Authentifizierungs-Credentials, zum Beispiel SAP Logon Tickets.

DirX Access kann bestehende Authentifizierungs-Authorities integrieren und so die existierende Authentifizierungsinfrastruktur nutzen.

Die Administratoren können für jede einzelne Web- oder Web-Service-Ressource oder für Ressourcen anderer Applikationen, die von DirX Access geschützt werden, die bevorzugte Authentifizierungsmethode festlegen. Auf diese Weise können sie separat für jede Ressource eine adäquate Sicherheitsstufe einstellen.

Administratoren können in DirX Access eine Rangfolge für die konfigurierten Authentifizierungsmethoden festlegen. Diese Rangfolge wird über sogenannte Assurance Levels festgelegt und kennzeichnet auf einer numerischen Werteskala, wie sicher die Authentifizierungsmethoden im Verhältnis zueinander sind. Diese Assurance Levels können als Bedingungen für die Autorisierung genutzt werden. Beispielsweise kann für den Zugriff auf eine sicherheitskritische Ressource eine Policy mit dem Assurance Level 4 eingestellt werden, was bedeutet, dass ein Benutzer mit der sichersten Methode authentifziert sein muss, um den Zugriff auf die Ressource zu erhalten. Assurance Levels sind in der NIST Special Publication 800-63 definiert.

DirX Access stellt Step-Up Authentifizierung zur Verfügung, bei der eine stärkere Authentifizierungsmethode angefordert wird, wenn auf eine sicherheitskritischere Ressource zugegriffen wird.

Risikobasierte Authentifizierung

Bei der risikobasierten Authentifizierung wird der Zugriff auf Ressourcen durch eine Risikoanalyse abgesichert. Das Ergebnis der Risikoanalyse legt fest, welche Mindeststärke der Authentifizierung für den Zugriff auf die Ressource erfüllt sein muss. Ist der Benutzer bereits mit der geforderten Stärke authentifiziert, wird der Zugriff gewährt. Ansonsten wird eine stärkere Authentifizierung erzwungen. Die Risikoanalyse berücksichtigt benutzer- und kontextspezifische Daten.

Die Risiko-Analyse basiert auf zwei Konzepten:
- Auswertung von vordefinierten, statischen Bedingungen
- Berücksichtigung von Verlaufsdaten

Der DirX Access Data Collector sammelt dazu alle Daten, die Risiko-relevant sein können und speichert diese mit den Benutzerdaten.
Die gesammelten Daten werden nach jeder Authentifizierung weiter aktualisiert. Im Authentifizierungsprozess werden diese Daten sowohl zur Durchführung einer statistischen Analyse genutzt als auch als Basis für eine Verhaltensanalyse.

Die risikobasierte Authentifizierung vergleicht den Grad der Schutzwürdigkeit einer Ressource mit dem Risikograd des Zugriffs. Zur Vermeidung von Risiken wird eine Ressource mit DirX Access typischerweise mittels einer Authentifizierungsmethode geschützt, die einem bestimmten Schutzniveau entspricht.

Zur Umsetzung des beschriebenen Konzepts werden sogenannte Risikobedingungen genutzt, um eventuelle Bedrohungen zu erkennen. Folgende Parameter können in Risikobedingungen konfiguriert werden:
- Schutzbedarf für die Ressource
- IP-Adressbereiche
- Zeiträume, zum Beispiel typische Arbeitszeiten in einem Unternehmen wie zum Beispiel 6 bis 19 Uhr, montags bis freitags
- Eigenschaften des HTTP Protokoll Headers wie zum Beispiel Typ des Web Browsers
- Kundenspezifische Bedingungen, die als Plugins (Callouts) implementiert werden, zum Beispiel ein Callout zu einem Geolokationsdienst, der aus einer IP-Adresse einen geographischen Standort bestimmen kann.
- Anzahl von hintereinander fehlgeschlagenen Login-/Anmeldeversuchen
- Login-Intervall, d.h. der Zeitraum zwischen zwei Login-Aktionen
- Benutzerkontext, um auf Basis der vom DirX Access RBA Data Collector gesammelten Daten ein ungewöhnliches Verhalten des authentisierenden Benutzers festzustellen, zum Beispiel eine neue IP-Adresse, von der aus sich der Benutzer anmelden will.

Single Sign On und Session Management

Sobald Benutzer erfolgreich für eine mit DirX Access geschützte Ressource authentifiziert wurden, müssen sie nicht noch einmal authentifiziert werden, wenn sie anschließend eine andere Ressource in derselben Domäne nutzen wollen, die ebenfalls mit DirX Access geschützt ist, es sei denn, dass die Ressource eine Step-Up Authentifizierung erfordert. Der Authentifizierungsstatus eines authentifizierten Benutzers wird dabei über HTTP Cookie Header oder URL Rewriting weitergegeben.

DirX Access verwaltet Security Sessions, indem es Informationen über authentifizierte Benutzer-Identitäten verwaltet. Diese Informationen beinhalten die Authentifizierungsmethode, den Authentifizierungszeitpunkt, die Authentifizierungscredentials und andere Parameter, die dem Login-Ereignis zuzuordnen sind. DirX Access stellt eine Schnittstelle für Plug-Ins zur Verfügung, die Subjektattribute von externen Quellen holen können, um die Session-Information zu ergänzen.

Zusätzlich können Umgebungsinformationen in den authentifizierten Subjekten behandelt werden, zum Beispiel von lösungsspezifischen Sicherheitsumgebungen wie Informationen zum Trust-Level des Netzwerks oder zur Art des Gerätes, das genutzt wird.

Für jedes erfolgreiche Login wird eine neue Security-Session erzeugt. Eine Security-Session wird zwischen Web-Browsern und dem DirX Access Server aufgebaut, wobei ein Session-Identifikator benutzt wird, der auf die Informationen des authentifizierten Benutzers im Cache verweist.

Eine existierende Security-Session wird entweder durch ein explizites Logoff (initiiert durch den Benutzer), durch ein Timeout der Session, durch Idle Time-Out oder durch das Herunterfahren aller DirX Access Server in einem Serververbund beendet. In jedem dieser Fälle wird die zugesicherte Benutzerinformation, die im Cache gehalten wird, entwertet, so dass sie von den Web-Browsern nicht mehr genutzt werden kann.

Zu den weiteren Session-Management Eigenschaften von DirX Access gehören:
- SSO Session Augmentation: DirX Access ermöglicht anderen Anwendungen, den SSO-Zustand, der für authentifizierte Benutzer gepflegt wird, mit weiteren Informationen zu ergänzen, die für DirX Access opak sind. Diese Daten können abgefragt werden, sie können in Autorisierungsentscheidungen genutzt werden oder in SAML Assertions und Auditdaten berücksichtigt werden.
- SSO Callout-Schnittstellen für Plug-Ins, mit der andere Anwendungen über Session-relevante Ereignisse benachrichtigt werden können wie zum Beispiel Benutzer-Logout, Session Time-Out oder Idle Time-Out. Dies ist speziell dann nützlich, wenn andere Anwendungen applikationsspezifische Session-Informationen zum SSO-Zustand in DirX Access hinzufügen.
- SSO Session Korrelation zwischen mehreren Browsern: dies ermöglicht, den SSO-Zustand, der für authentifizierte Benutzer gepflegt wird, basierend auf Kriterien wie Benutzer-Identifikatoren und –Herkunft (zum Beispiel auf Basis der IP-Adresse des Benutzers) abzugleichen. Diese Eigenschaft ist optional und ermöglicht in DirX Access die Zuweisung des gleichen SSO-Zustands zu Benutzersessions, die über verschiedene Frontends angelegt wurden.

Identity Federation und föderierte Authentifizierung

Identity Federation ist ein Menge von Standards und Technologien, mit denen es Partnerorganisationen ermöglicht wird, eine Vertrauensbeziehung bezüglich ihrer jeweiligen Sicherheitsrichtlinien/-infrastrukturen einzurichten und dann auf Basis der Vertrauensbeziehung Zugriffe auf Ressourcen zu gewähren oder zu verweigern.

Identity Federation ermöglicht die gemeinsame, sichere Nutzung von digitalen Identitäten und Login-Sessions über mehrere Security-Domänen hinweg. Es erleichtert die sichere und nahtlose Online-Zusammenarbeit, indem es den sicheren Zugriff auf Partner-Ressourcen ermöglicht, ohne dass die Benutzer erneut authentifiziert werden müssen, und erlaubt den Partnern, Identitätsinformationen gegenseitig zu vertrauen und gemeinsam für die Authentifizierung und Autorisierung zu nutzen, ohne sie bei jedem einzelnen Partner erzeugen und verwalten zu müssen.

Identity Federation mit DirX Access kann

- die Kosten und Komplexität von Online-Zusammenarbeit senken, indem es die Notwendigkeit für das Vorhalten mehrerer Benutzerprofile eliminiert
- durch das domänenübergreifende Single Sign-On für positive Benutzererfahrungen sorgen
- die Produktivität verbessern, indem es einen sicheren, komfortablen Zugriff auf die Ressourcen von Partnern einer Trustbeziehung ermöglicht
- mit anderen standardkonformen Federation-Lösungen zusammenarbeiten.

DirX Access erweitert mit Identity Federation seine wesentlichen Services für Authentifizierung und Autorisierung für den Einsatz in virtuellen Unternehmen.

Föderierte Authentifizierung bedeutet, dass Informationen über einen Authentifizierungszustand einer Identität von einem Identity Provider zu einem Service Provider oder Relying Party in einer anderen Domäne übertragen werden.

DirX Access unterstützt Identity Federation sowohl via SAMLV2.0 als auch via OpenID Connect 1.0, das Authentifizierungsfunktionalität über das OAuth 2.0 Protokoll bereitstellt.

Im Gegensatz zur initialen Authentifizierung erfordert die föderierte Authentifizierung nicht, dass jeder Benutzer einen zugehörigen Account auf der Service Provider Seite hat. Stattdessen weist der Identity Provider den Benutzern typischerweise Rollen zu und der Service Provider erlaubt bzw. verweigert den Zugriff entsprechend der Rolle in der Security-Assertion. Auf diese Weise werden sämtliche Informationen, die zur Durchführung der Authentifizierung benötigt werden (wie Identitätsinformationen, Anmeldedaten, etc.), lokal beim Identity Provider verwaltet, die endgültige Zugriffsentscheidung verbleibt jedoch in der alleinigen Verantwortung des Service Providers.

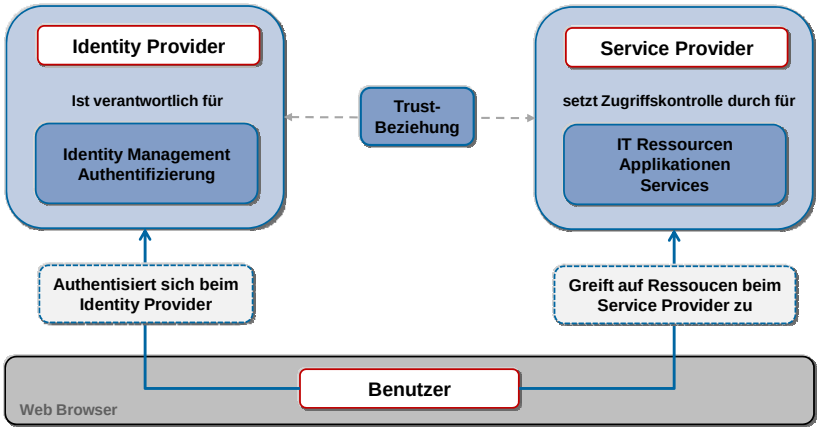

Abb. 2: DirX Access – SAML Federation Modell

Auch für die föderierte Authentifizierung wird Single Sign-On zur Verfügung gestellt.

SAML-basierte Federation

Im Fall von SAML-basierter Identity Federation nutzt DirX Access die Security Assertion Markup Language (SAML) Assertions, um Identitäten in föderierten Transaktionen zu repräsentieren.

DirX Access unterstützt beide SAML V2.0 Federation-Szenarien:

- Service Provider-/SP-initiiert: In diesem Fall versucht der Benutzer auf eine Ressource in der föderierten Domäne zuzugreifen, ohne vorher authentifiziert zu sein. Die föderierte Domäne leitet den Benutzer zur Authentifizierung zum Identity Provider um. Sobald die Authentifizierung erfolgreich durchgeführt wurde, wird der Benutzer transparent zur Ziel-Site zurückgeleitet, wo die Autorisierung stattfindet und schließlich der Zugriff auf die gewünschte Ressource.
- Identity Provicer-/IdP-initiiert: In diesem Fall wird der Benutzer zuerst in der lokalen Domäne authentifiziert und fordert dann einen Service oder eine Ressource in der föderierten Domäne an.

In beiden Szenarien kann DirX Access sowohl den Identity Provider repräsentieren, der den Benutzer authentifiziert, als auch den Service Provider, dem die Ressource gehört und der der Authentifizierung des Identity Providers vertraut.

DirX Access unterstützt die folgenden SAML V2.0 Profile, zugehörigen Message-Protokolle und Bindings gemäß dem SAML V2.0 Conformance Requirements Dokument:

- Web Browser SSO Profile mit AuthnRequest Message vom SP zum IdP via HTTP Redirect oder HTTP POST Binding
- Web Browser SSO Profile mit IdP Response Message zum SP via HTTP POST oder HTTP Artifact Binding inklusive Unsolicited Responses (IdP first)
- Identity Provider Discovery Profile mit Cookie Setter und Cookie Getter Messages via HTTP Binding
- Single Logout Profile mit LogoutRequest und LogoutResponse Messages via HTTP Redirect, HTTP POST, HTTP Artifact oder SOAP Binding
- Artifact Resolution Profile mit ArtifactResolve und ArtifactResponse Message via SOAP Binding
- Assertion Query/Request Profile mit Authentication Query, Attribute Query, Authorisation Decision Query und Request for Assertion by Identitfier Messages via SOAP Binding
- Basic Attribute Profile
- X.500/LDAP Attribute Profile
- UUID Attribute Profile
- XACML Attribute Profile

DirX Access unterstützt die folgenden SAML Protokolle:

- Authentication Request Protokoll
- Artifact Resolution Protokoll
- Single Logout Protokoll
- Assertion Query/Request Protokoll mit Authentication Query, Attribute Query, Authorisation Decision Query und Request for Assertion by Identitfier Elementen

Request/Response-Objekte können signiert werden (enveloped XML-Signatur).

DirX Access unterstützt SAML Assertions mit folgenden Inhalten:

- Authentication Statements
- Attribute Statements
- Authorization Decision Statements

Assertion-Objekte und Protokoll-Objekte können signiert werden (enveloped XML-Signatur). SAML Assertions, Namelds und Attribute können verschlüsselt werden.

DirX Access kann Umgebungsinformationen wie Informationen zum Trust-Level des Netzwerks oder zur Art des Gerätes, das genutzt wird, in die SAML Assertions integrieren.

DirX Access unterstützt den Import und den Export von SAML Metadata zur beidseitigen Konfiguration zwischen einem Identity Provider und einem Service Provider.

SAML Proxying

DirX Access unterstützt SAML Proxying basierend auf der SAML V2.0 Spezifikation, d.h. Identity Provider können eine Authentifizierungsanfrage eines Service Providers an einen anderen Identity Provider weiterleiten, der den Benutzer authentifizieren kann. Dadurch wird es möglich, die initiale Benutzerauthentifizierung, von einem lokalen SAML Identity Provider zu einem externen Identity Provider zu delegieren.

Ein Proxying IdP ist eine Kombination eines klassischen SAML IdP, der die Authentifizierung durchführt und der insbesonders den SAML SingleSignOnService bereitstellt, und eines klassisschen SP, der den SAML AssertionConsumerService bereitstellt.

SAML Proxying in DirX Access unterstützt folgende Szenarien:

- Mehrere Proxying IdPs können zwischen dem Service Provider und dem eigentlichen IdP konfiguriert werden
- Ein Proxying IdP kann mit mehreren Identity Provider und/or mehreren Service Providern konfiguriert werden, so dass der Proxying IdP als Drehscheibe (Hub, Bridge, Gateway) in einem Identity Federation Verbund eingesetzt werden kann.

Just-in-Time Provisioning

DirX Access ermöglicht Just-in-Time Provisioning, auch JIT Provisioning genannt, ein Modell für dynamisches User Provisioning in SAML-basierten Federation-Umgebungen. Es zielt auf (Cloud) Federation-Szenarien, in denen (Cloud) Service Provider Identitätsdaten von einem Identity Provider als Voraussetzung zur Genehmigung des Zugriffs auf ihre (Cloud) Dienste benötigen.

Just-in-Time Provisioning ist im Wesentlichen eine Lösung auf Seite des Service Providers. Es ermöglicht diesem, Benutzerkennungen direkt einzurichten, wenn der Benutzer sich erfolgreich mittels des SAML Federation Protokolls mit einer SAML Assertion authentifiziert, die von einem vertrauenswürdigen Identity Provider ausgestellt wurde. Es nutzt die Attribute der vom Identity Provider übermittelten SAML Assertion, um Benutzer in seinem Benutzer-Directory anzulegen. Just-in-Time Provisioning ist für Anwendungsfälle nützlich, bei denen die Benutzer nicht im Voraus beim Service Provider bekannt sein müssen, wie zum Beispiel bei Supply Chain Portalen, bei gemeinsamen Projekten oder bei vielen Cloud-Anwendungen.

DirX Access unterstützt sowohl Pull- als auch Push-basierte JIT Provisioning Szenarien:

- Im Push-Modell erzeugt der Service Provider eine Benutzerkennung mittels der Identitätsdaten aus der vom Identity Provider übermittelten SAML Assertion. DirX Access unterstützt Push-basiertes JIT Provisioning mit seinem eigenen Benutzer-Directory und mit jedem SAML SP, der JIT Provisioning unterstützt, zum Beispiel Salesforce.com.
- Im Pull-Modell entscheidet der Service Provider, wann und wie er Identitätsdaten vom Identity Provider anfordert, von dem er die SAML Assertion empfangen hat. Dazu fordert er zuerst vom Identity Provider die erforderlichen Identitätsdaten an und erzeugt dann die Benutzerkennung mittels der Identitätsdaten, die in der SAML Assertion enthalten sind sowie mittels der zusätzlich angeforderten Daten.

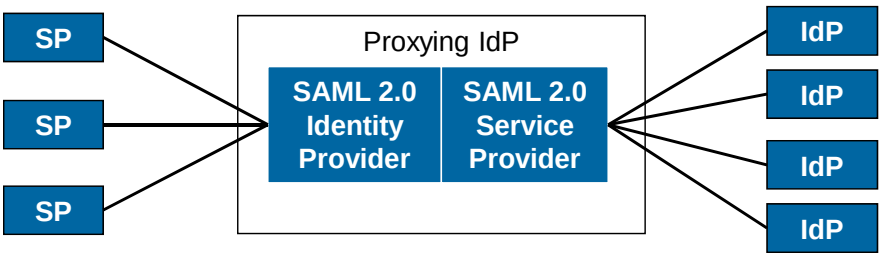

Abb. 3: DirX Access Beispiel - SAML Proxying IdP in einem Hub/Spoke Szenario

Nachgewiesene SAML V2.0 Interoperabilität

DirX Access hat im Jahr 2009 die SAML V2.0 Interoperabilitätstests der Liberty Alliance bestanden. DirX Access hat am dritten Liberty Interoperable™ Full-Matrix Test-Event für SAML V2.0 zusammen mit acht anderen Produkten verschiedener Hersteller teilgenommen und demonstriert, dass es die strengen Testkriterien für ein offenes, sicheres und die Privatsphäre schützendes föderiertes Identity Management erfüllt.

Identity Federation und Cloud-Computing

DirX Access stellt Single Sign-On für Cloud-basierte Applikationen oder für Software as a Service (SaaS) zur Verfügung, um den Zugriff darauf kostengünstig und zuverlässig zu sichern. Für die Authentifizierung der Benutzer für den Zugriff auf die externen Applikationen (SaaS oder Cloud-basiert) werden Federation-Standards wie SAML genutzt.

Vorkonfigurierte SAML Service Provider

DirX Access unterstützt vorkonfigurierte SAML Service Provider. Diese Funktionalität ermöglicht es Administratoren, auf einfache Art eine Verbindung zwischen einem DirX Access Identity Provider und bekannten Cloud Service Providern wie Google Apps, Citrix ShareFile, Microsoft Office 365 und Salesforce.com einzurichten, für die DirX Access entsprechende Konfigurationen standardmäßig mitliefert. Zudem besteht die Möglichkeit, Provider-Instanzen zu parametrisieren und kundenspezifische Templates für andere vorkonfigurierte Service Provider oder Identity Provider zu erzeugen.

Identity Federation mit OpenID Connect

DirX Access unterstützt auch die Core Spezifikation des OpenID Connect 1.0 Standards. OpenID Connect 1.0 ist ein Identity-Layer, das auf dem OAuth 2.0 Protokoll aufsetzt. Es ermöglicht Clients, die Identität des Benutzers basierend auf der Authentifizierung, die von einem Authorization Server durchgeführt wurde, zu verifizieren und zusätzliche Informationen über den Benutzer basierend auf REST-Schnittstellen zu erhalten.

Die Abbildung 4 zeigt ein Single Sign-On Szenario basierend auf OpenID Connect, bei dem sich die Benutzer mit ihren sozialen Identitäten bei Systemen wie Google oder Salesforce authentifizieren, um auf IT-Ressourcen zuzugreifen, die mittels DirX Access geschützt werden. In diesem Szenario wird DirX Access für die Authentifizierung über OpenID Connect eingesetzt sowie für die Autorisierung des Zugriffes zu den IT-Ressourcen in einem Service Provider Einsatzfall.

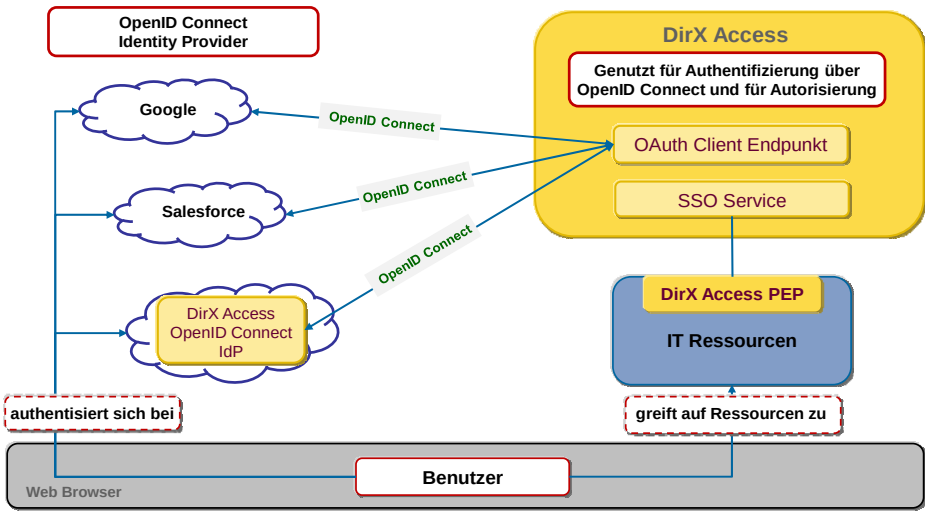

Abb. 4: Single Sign-On mit sozialen Identitäten basierend auf OpenID Connect

Federation mit Microsoft SharePoint

DirX Access ermöglicht Identity Federation mit Microsoft SharePoint mittels Unterstützung des WS-Federation Passive Requestor Profiles zur Authentifizierung in SharePoint. Andere Anwendungen, die WS-Federation Passive Requestor Profile unterstützen, können auf die gleiche Art und Weise angeschlossen werden.

In diesem Szenario unterstützt Microsoft SharePoint in seiner Rolle als Service Provider die Authentifizierung durch einen vertrauenswürdigen Identity Provider.

DirX Access implementiert die erforderlichen Funktionen sowohl des Identity Providers als auch des Security Token Service für die Nutzung des WS-Federation. Passive Requestor Profiles.

Autorisierung und Entitlement Management

Mit DirX Access wird die Autorisierungs-Funktionalität als ein externer, zentraler, Policy-basierter Service für die Zugriffskontrolle bereitgestellt, der es ermöglicht, einen umfassenden Satz von Zugriffskontrollpolicies festzulegen, und basierend auf diesen Policies den Zugriff auf die angeforderten Ressourcen zu gewähren oder abzulehnen.

Basierend auf dem XACML-Standard (eXtensible Access Control Markup Language), der von der Organization for the Advancement of Structured Information Standards (OASIS) standardisiert wurde, können Zugriffspolicies so festgelegt werden, wie sie sich für die Einsatzumgebung am besten eignen.

Zum Beispiel werden beim Rollen-basierten Zugriffskontrollmodell (RBAC, Role-Based Access Control) die Zugriffspolicies basierend auf den Rollen der Benutzer festgelegt, während bei der Attribut-basierten Zugriffskontrolle (ABAC, Attribute-Based Access Control) die Zugriffspolicies basierend auf Attributwerten der Benutzer festgelegt werden und bei der Discretionary Zugriffskontrolle (DAC, Discretionary Access Control), die Zugriffspolicies vom Eigentümer des Objekts festgelegt werden. Der Eigentümer entscheidet, wer auf das Objekt zugreifen darf und wer welche Rechte hat.

Die Policy-basierte Autorisierung hat viele Vorteile. Die Definition und Verwaltung von Zugriffskontrollpolicies erfolgt unabhängig von der einzelnen Applikation und die Notwendigkeit für die Implementierung einer Zugriffskontrollogik für jede einzelne Applikation kann vermieden werden. Die Erzeugung von Zugriffskontrollpolicies wird so eine einmalige Aufgabe statt einer immer wiederkehrenden, die Administration von Zugriffsrechten über mehrere Web-Applikationen und –Ressourcen hinweg wird vereinfacht und die konsistente Anwendung von Zugriffsrechten sowie die konsistente Durchsetzung von Sicherheitsrichtlinien über die Zeit wird ermöglicht.

DirX Access nutzt XACML V1.x/2.0/3.0 als zugrundeliegende Autorisierungstechnologie und unterstützt folgende Autorisierungsmodelle:

- Frei wählbare, durch die Applikation definierte Autorisierungsmodelle; jedes Autorisierungsmodell, das als gültiges XACML-Objekt formuliert werden kann, kann genutzt werden, d.h. der Policy-Inhalt ist formfrei, sofern die geltenden Syntaxanforderungen erfüllt werden.
- Ein RBAC-basiertes Autorisierungsmodell, das Zugriffe zu Ressourcen von Web Services und Web-Applikationen als auch zu Ressourcen anderer Anwendungen auf Basis der Rolle des anfordernden Benutzers in der Organisation gewährt oder ablehnt. Administratoren definieren die Business-Rollen, die in der Organisation genutzt werden, und legen auf Basis der geschäftlichen Notwendigkeiten die Ressourcen fest, für die der Zugriff für die jeweilige Rolle erlaubt werden soll. Dieses Autorisierungsmodell wird auf Basis des RBAC-Profiles von XACML formuliert, das heißt, dass die Policies, die in diesem Autorisierungsmodell formuliert werden können, die Anforderungen dieses speziellen Profils erfüllen müssen.

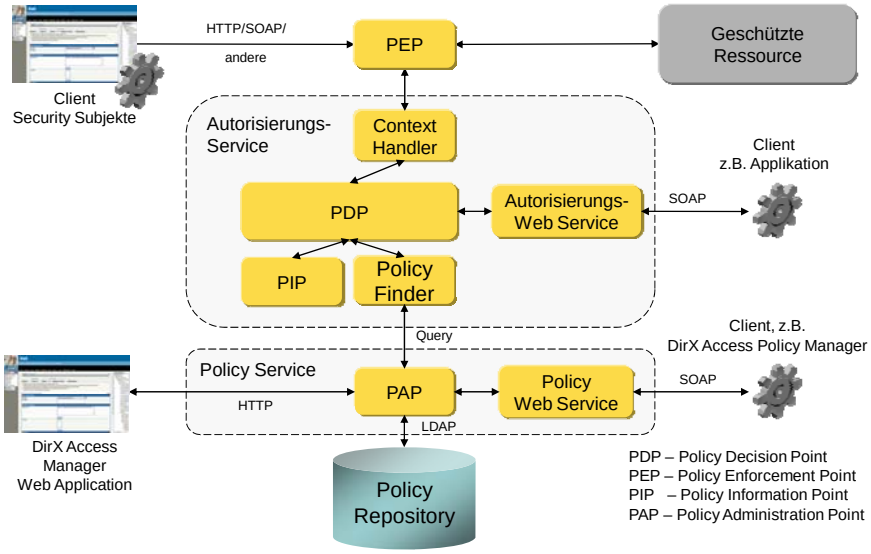

Abb. 5: DirX Access – XACML-basiertes Autorisierungssystem

Innerhalb von DirX Access wird die Autorisierung von folgenden Komponenten bereitgestellt (siehe Abbildung 5):

- PEPs (Policy Enforcement Points), die als Plugins zu Web Servern, Web Application Servern oder anderen Applikationen eingesetzt werden, verarbeiten die Zugriffsanfragen, senden Anfragen für Autorisierungsentscheidungen an den PDP (siehe unten) und stellen die Autorisierungsentscheidung ihrer Umgebung zur Verfügung. Einige PEPs setzen die Autorisierungsentscheidung selbst durch, andere PEPs informieren nur ihre Umgebung über die Entscheidung des PDP.
- PDPs (Policy Decision Points), die als Teil des DirX Access Servers bereitgestellt werden, liefern Autorisierungsentscheidungen für Zugriffsanfragen der PEPs. Ihre Entscheidungen basieren auf den Autorisierungspolicies, die sie von PAPs erhalten.
- PAPs (Policy Administration Points) sind Autorisierungs-Policy-Instanzen, die es den Administratoren ermöglichen, Autorisierungspolicies zu erzeugen, zu pflegen und zur Verfügung zu stellen. Im DirX Access Server wird der PAP durch den Policy Service repräsentiert. Dieser Service kann mittels des DirX Access Managers, des DirX Access Provisioning Web Service (für RBAC-konforme Autorisierungspolicies), über die DirX Access Policy Web Services (für andere Policies) oder mittels des DirX Access Policy Manager genutzt werden. Die Authentifizierung und die Autorisierung für den Zugriff auf die PAPs wird mit den DirX Access-eigenen Mitteln durchgeführt.
- PIPs (Policy Informations Points) können genutzt werden, um auf Informationen über die Anwendungsumgebung zuzugreifen, die für die Berechnung von Policy-Entscheidungen erforderlich sind. Zudem können PIPs Informationen über die Subjekte oder die Ressourcen bereitstellen, die bei einer Anfrage betroffen sind.

DirX Access unterstützt die dynamische Zugriffskontrolle/Autorisierung mit Unterstützung sogenannter Attribute Finder, die dem PDP weitere konfigurierbare Informationen für die Zugriffsentscheidungen zur Verfügung stellen. Sämtliche Informationen, die in der authentifizierten Session (JAAS-Subjekten) enthalten sind, können genutzt werden, zum Beispiel die LDAP-Attribute des Benutzers, Attribute aus SAML-Assertions, OAuth-Benutzerprofildaten, Anwendungs- und umgebungsspezifische Attribute, die vom PEP zum Server übertragen werden, zum Beispiel Informationen zum genutzten Gerät oder zur genutzten Anwendung, etc.

Zusätzlich kann DirX Access in Echtzeit auf Änderungen von Benutzerdaten reagieren, zum Beispiel durch Entzug von Zugriffsrechten, wenn entsprechende Benutzerattribute geändert werden.

Föderierte Autorisierung

DirX Access unterstützt das OAuth 2.0 Authorization Framework und eine Reihe von OAuth 2.0 basierten Standards wie die Spezifikationen für User-Managed Access (UMA) 2.0, OAuth 2.0 Token Introspection (RFC 7662) and OAuth 2.0 Dynamic Client Registration Protocol (RFC 7591).

OAuth 2.0

DirX Access unterstützt den OAuth 2.0 Authorization Framework für die Autorisierung in Federation Szenarien. OAuth definiert ein Ressourcen-bezogenes Autorisierungsprotokoll, dass es Ressourcen-Eigentümern ermöglicht, Zugriffsrechte für ihre Ressourcen zu delegieren.
Dadurch wird es möglich, Ressourcen über Organisationsgrenzen hinweg gemeinsam nutzen zu können, ohne die Anmeldedaten mitteilen zu müssen. Um diesen Anwendungsfall zu unterstützen, stellt DirX Access sowohl OAuth Client Funktionalität als auch OAuth Server Funktionalität bereit.

DirX Access kann unabhängig oder in Verbindung mit einem Browser-basiertem Single Sign-On entweder für einen Identity Provider Einsatz oder für einen Service Provider Einsatz konfiguriert werden:

- In einem Service Provider Einsatz fordert der OAuth Client Federation Endpunkt ein Access Token an und nutzt dieses, um auf die geschützte Ressource zuzugreifen.
- In einem Identity Provider Einsatz kann der OAuth Server Federation Endpunkt genutzt werden, um den Benutzer zu authentifizieren und das Access Token mit den zugehörigen Benutzerinformationen auszustellen.

User-Managed Access (UMA)

DirX Access unterstützt die folgenden für UMA relevanten Spezifikationen:

- User-Managed Access 2.0 Grant for OAuth 2.0 Authorization – eine Methode für einen Client, Zugriff auf eine geschützte Ressource zu erhalten, asynchron vom Zeitpunkt, zu dem der Ressourcen-Eigentümer den Zugriff autorisiert hat.
- Federated Authorization for User-Managed Access 2.0 – eine Methode für UMA Authorization und Resource Server in einem Ressourcen-Eigentümer Kontext lose gekoppelt oder föderiert zu werden.

Benutzerverwaltung

Die initiale Authentifizierung von Benutzern erfordert, dass die Identitäten in einem LDAP-Directory verwaltet werden. Dies kann ein extern verwaltetes Directory mit einem eigenen Schema sein, z.B. inetOrgPerson, oder ein LDAP-Directory, das unter der administrativen Kontrolle von DirX Access steht, das DirX Access Benutzer-Directory.

Im ersten Fall erfolgt die Benutzerverwaltung mittels der entsprechenden externen Benutzerschnittstellen und Tools. DirX Access kann beliebige LDAP-Attribute für seine Authentifizierungs- und Autorisierungszwecke nutzen.

Wenn DirX Access die Benutzerverwaltung selbst durchführt, kann der DirX Access Manager genutzt werden, um die Endbenutzer-Accounts zu administrieren. Dazu stellt der DirX Access Manager eine intuitiv zu bedienende Benutzerschnittstelle zur Verfügung (siehe auch im Abschnitt Administration in diesem Dokument).

Sobald die Authentifizierung erfolgt ist, können alle Attribute aus dem Benutzereintrag in Federation- oder Autorisierungsszenarien (Ausstellen von SAML-Assertions, Freigeben von OAuth-Benutzerprofildaten, Auswertung von Autorisierungspolicies, etc.) genutzt werden. Dazu können Daten aus beliebigen LDAP-Verzeichnissen herangezogen werden.

Bei föderierter Authentifizierung kann DirX Access Benutzer-Accounts auf der Service Provider Seite im DirX Access Benutzer-Directory mittels Just-in-time Provisioning direkt basierend auf den Informationen in den SAML-Tokens erzeugen.

DirX Access stellt einen SPML-basierten Provisioning Web Service zur Verfügung, um Benutzer-Accounts und deren Attribute im DirX Access Benutzer-Directory zu provisionieren. Sowohl SPML V1.0 als auch V2.0 werden unterstützt.

Für komplexere Aufgaben wie die Zuweisung von Benutzerattributen und Berechtigungen, die Integration mehrerer unterschiedlicher Directories, Benutzerdatenbanken und Applikations-spezifischer Directories wird empfohlen, Identity Management Systeme wie beispielsweise DirX Identity einzusetzen. DirX Identity stellt auch eine Workflow-basierte Selbst-Registrierung für die Benutzer und Funktionen für die Selbstverwaltung durch die Benutzer sowie viele weitere Identity Management Funktionen zur Verfügung.

Policy Management

Das Policy Management in DirX Access stellt die Funktionen zum Erzeugen, Ändern, Löschen and Anzeigen von Authentifizierungs- und Autorisierungspolicies auf Basis des OASIS XACML-Standards zur Verfügung.

In DirX Access gibt es administrative Policies, die die Administration von DirX Access regeln, und Business-Policies, die den Zugriff von Benutzern zu den geschützten Ressourcen regeln.

Authentifizierungspolices setzen die Anwendung von spezifischen Authentifizierungsmethoden für die jeweilige Ressource durch.

Autorisierungspolicies wenden Autorisierungsregeln an, die die Zugriffe auf geschützte Ressourcen steuern. Feingranulare Autorisierungspolicies ermöglichen es, das für die Autorisierung benötigte Granularitätslevel festzulegen. Sie berücksichtigen die Eigenschaften der betroffenen Ressourcen (zum Beispiel deren Sicherheitseinstufung) und der anfordernden Subjekte (wie Benutzernamen, Gruppenmitgliedschaften oder Rollenzuordnungen), um den Zugriff zu Ressourcen zuzulassen oder nicht autorisierte Zugriffe zu verhindern.

Access Tester

Autorisierungspolicies können mit dem Access Tester aus der DirX Manager Tool-Umgebung getestet werden. Dieser ermöglicht es Administratoren, Zugriffe von Benutzern oder Rollen auf Basis der aktuellen Policy zu simulieren, um zu sehen, was passieren wird und ob die Konfiguration das gewünschte Ergebnis liefert.

Schutz von Web-Applikationen

Access Management Lösungen waren ursprünglich darauf ausgerichtet, den Zugriff zu Web-Applikationen und Web-Inhalten zu sichern, die aus eBusiness-, eGovernment- und Online-Portalen zugänglich sind. Dazu stellt DirX Access Funktionen für externe, zentrale und Policy-basierte Authentifizierungs- und Autorisierungs-Dienste, Identity Federation und Single Sign-on zur Verfügung, um einen sicheren, komfortablen und vertrauenswürdigen Zugriff zu mehreren Web-Applikationen mit einer einzigen Authentifizierung zu ermöglichen.

DirX Access PEPs, die Web-Applikationen schützen, können in Protokollstackerweiterungs-PEPs, Agent-PEPs und Applikations-PEPs klassifiziert werden. Des Weiteren können kundenspezifische PEPs mit Hilfe des Client SDKs oder mittels der DirX Access Web Services erstellt werden.

Protokollstackerweiterungs-PEPs werden in Protokollstacks eingesetzt. Die bekanntesten Beispiele sind die HTTP-Stack PEPs (Web-PEPs) wie die PEPs für Apache Web Server, Apache Tomcat oder Microsoft Internet Information Server. Sie integrieren mit den nachgelagerten Applikationen, die sie schützen, hauptsächlich mittels Header Injection. Damit können den Applikationen Daten aus verschiedenen Quellen zur Verfügung gestellt werden, zum Beispiel diverse Session- und/oder Benutzerattribute sowie Daten aus beliebigen LDAP-Verzeichnissen.

Agent-PEPs nutzen die vorhandenen Schnittstellen der Web oder Application Server, um die Anwendungen zu schützen, die in diesen Servern laufen. Der DirX Access Agent PEP für den Microsoft Internet Information Server (IIS) stellt Event Handler zur Verfügung, die die Authentifizierungs- und Autorisierungsanfragen des IIS Servers bearbeiten.

Applikations-PEPs können für Applikationen zur Verfügung gestellt werden, die standardisierte oder veröffentlichte Schnittstellen dafür zur Verfügung stellen. Ein wichtiges Beispiel sind Servlet-Applikationen, die individuell durch den DirX Access Servlet Filter PEP geschützt werden können. Weitere Beispiele sind Cloud-Anwendungen, die in Cloud-Applikationsplattformen wie zum Beispiel Cloud Foundry arbeiten. Diese Applikationen können durch den DirX Access Cloud Foundry PEP geschützt werden. Andere Applikationen, die derartige Integrationsschnittstellen nicht zur Verfügung stellen, können mittels kundenspezifisch entwickelter PEPs geschützt werden, die mit dem DirX Access Client SDK erstellt werden.

Schutz von Legacy-Anwendungen

Die Nachfrage nach Online-Zusammenarbeit, die Anforderungen für erhöhte betriebliche Effizienz und für den Zugriff zu Business-Ressourcen rund um die Uhr führen dazu, dass Unternehmen den Zugriff zu ihren Legacy-Anwendungen vermehrt online zur Verfügung stellen. DirX Access bietet die Mittel, diese Legacy-Anwendungen mit den gleichen externen, zentralen und Policy-basierten Authentifizierungs- und Autorisierung-Services zu sichern, die für die neueren Web-fähigen Anwendungen eingesetzt werden.

DirX Access unterstützt Applikations-PEPs, die mit bestimmten Anwendungen integriert werden können und diese schützen. Abhängig vom Integrationsmechanismus können diese PEPs klassifiziert werden als:

- Applikations-Source PEPs, d.h. kundenspezifische PEPs, die die Client-SDK-Methoden von DirX Access nutzen, die in den Source-Code der Applikationen integriert werden,
- PEPs, die die Applikationen ergänzen: kundenspezifische oder Standard PEPs, zum Beispiel AOP-basierte PEPs (Aspekt-orientierte Programmierung).

Legacy-Applikationen können PEPs und PDPs als ihr Access Management System nutzen. Die PEPs und PDPs stellen zentral externe Methoden für die Kontrolle des Zugriffs zu diesen Applikationen zur Verfügung, so dass diese Access Management Funktionen nicht in jeder Applikation einzeln implementiert werden müssen.

Security Web Services

Das Thema, Applikations-spezifische Sicherheitsfunktionalität aus den Applikationen auszulagern und zu zentralisieren, betrifft auch Web Services-basierte Service-orientierte Architekturen (SOAs). Wenn Applikationen als Web Services ablaufen sollen, stellt sich die Frage, wie die individuelle (und normalerweise einzigartige) Sicherheitslogik verwaltet wird, die in jeder einzelnen Applikation vorhanden ist.

DirX Access stellt sich diesen Herausforderungen und stellt seine Sicherheitsfunktionen in Form von Standard Web Services zur Verfügung, die in Web Service-basierten Service-orientierten Architekturen (SOA) eingesetzt werden können. Auf diesem Weg können Unternehmen Sicherheitslogik hinzufügen, die von jedem Business-Service in der Web Service-basierten Service-orientierten Architektur genutzt werden kann.

DirX Access stellt standardmäßig die folgenden Web Services zur Verfügung:

- Authentifizierungs- und SSO Web Service: ein Web Service, der Authentifizierungs- und Single Sign-On-Funktionalität zur Verfügung stellt
- Autorisierungs-Web Service: ein Web Service, der Autorisierungsentscheidungen und –tests basierend auf dem OASIS XACML-Standard durchführt
- Policy Web Service: Ein Web Service, der die Verwaltung und die Abfrage von Autorisierungs-Policies basierend auf dem OASIS XACML-Standard durchführt
- Federation Web Service: ein Web Service, der die Ausstellung von SAML-Assertions und die OASIS WS-Trust STS-Funktionalität (Security Token Service) zur Verfügung stellt
- Provisioning Web Service: ein Web Service, der es ermöglicht, DirX Access mit Benutzern, Gruppen und Organisationseinheiten zu provisionieren, und die Zuweisung dieser Objekte zu Rollen zu steuern.
  Der Provisioning Web Service basiert auf dem OASIS SPML V1.0 und V2.0 Standard
- Konfigurations-Web Service: ein Web Service, der zur Konfiguration des DirX Access Systems genutzt wird.

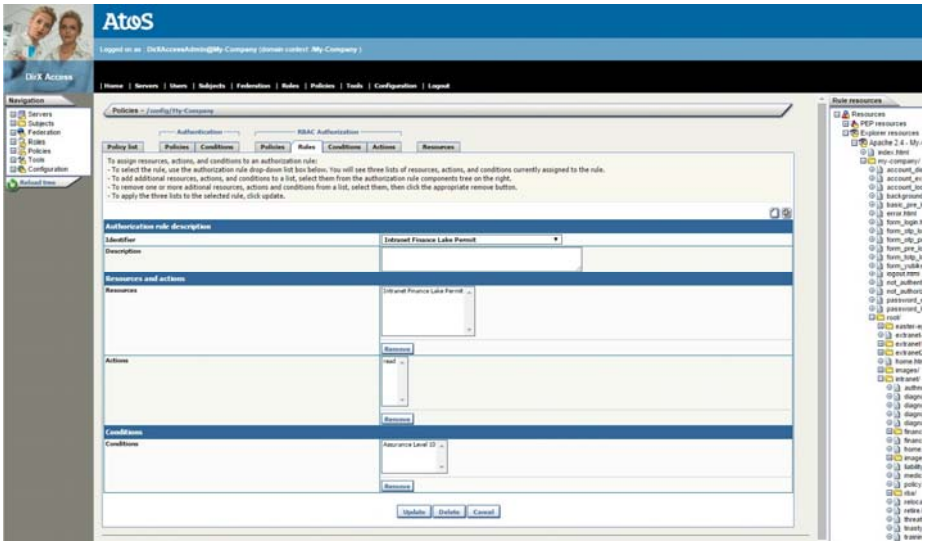

Abb. 6: DirX Access Manager – Beispiel der Administrationsoberfläche

Zusätzlich stellt DirX Access Client Services zur Verfügung, die Funktionen wie DirX Access Konfigurationsmanagement, Sessionmanagement, Authentifizierung und Autorisierung bieten. Diese Client Services basieren auf REST-Prinzipien mit Standard Create, Read, Update, Delete (CRUD) Zugriff auf die DirX Access Business Services. Sie nutzen das von OASIS standardisierte Open Data Protocol (OData) V4.0.

Administration

Administrationszuständigkeiten im Unternehmen spiegeln oftmals die Geschäftsstruktur wieder, so dass die Unternehmen die Verwaltung ihrer Benutzer, ihrer Benutzergruppen und der Policies für Ressourcenzugriffe denjenigen Personen zuweisen können, die mit den Notwendigkeiten ihres Geschäftsbereichs vertraut sind. DirX Access stellt Mittel zur flexiblen, sicheren Delegation von Administrationsrechten zur Verfügung, um auf temporäre Personalwechsel, auf Änderungen der Organisation oder der Prozesse reagieren zu können und ein agiles Unternehmen zu unterstützen.

DirX Access stellt Web-basierte Administrationstools zur Verfügung. Administrationsvorgänge können parallel ablaufen, so dass Zugriffspolicies schnell und effizient in der Organisation zum Einsatz gebracht werden können. DirX Access stellt grafische Resource Explorer zur Verfügung, die die zu schützenden Ressourcen einfach und schnell auffinden und registrieren können. Für den Fall, dass komplexere Identity Management- und Provisioning-Funktionen benötigt werden, kann DirX Access nahtlos mit DirX Identity integriert werden oder mit anderen Identity Management Lösungen zusammenarbeiten.

Die Zugriffskontrolle für die Administration nutzt die gleichen Authentifizierungs- und Autorisierungsmechanismen wie die Zugriffskontrolle für die Ressourcen der Organisation.

Die Administration von DirX Access wird mittels des DirX Access Managers, einem Web-basierten Administrationstool durchgeführt (siehe Abbildung 6). Die Administratoren können mit dem DirX Access Manager eine Reihe von Aufgaben ausführen wie:

- Erzeugen von Business-Rollen
- Festlegen von Benutzern, Gruppen und Organisationseinheiten, die Zugriff auf geschützte Ressourcen anfordern und Importieren von existierenden Benutzen aus externen Datenhaltungen
- Erzeugen von Authentifizierungspolicies durch Nutzung eines Ressourcen-Baums
- Konfiguration von Risikobedingungen und zugehörigen Data Collectors
- Erzeugen von Autorisierungsregeln und –policies unter Nutzung des Ressourcen-Baums
- Festlegen von Autorisierungsbedingungen, wie zulässige Tageszeit, Authentifizierungsmethode, Sicherheitsstufe oder erlaubte IP-Adressen für den Zugriff
- Zuweisung von Policies zu Rollen
- Zuweisung von Benutzern, Gruppen und Organisationseinheiten zu Rollen
- Konfiguration der internen Repräsentation von authentifizierten Subjekten
- Konfiguration der SAML Assertions von authentifizierten Subjekten
- Konfiguration der Federation
- Konfiguration der Server

- Konfiguration der PDPs
- Konfiguration der PEPs und Resource Explorer

Um Zugriffsrechte effizient festlegen und durchsetzen zu können, müssen DirX Access die zu schützenden Ressourcen bekannt gemacht werden.

Dazu dienen die Resource Explorer, die die Web und Applikations-Server, auf denen sie eingesetzt sind, absuchen und die dort verfügbaren Ressourcen auflisten, wie zum Beispiel Web-Seiten, Servlets, Beans oder Beans-Methoden. Wenn Ressourcen von den Explorer-Agenten entdeckt werden, werden sie zum hierarchischen Ressourcen-Baum im DirX Access Manager hinzugefügt. Diese automatische Erkennung von Ressourcen reduziert die Notwendigkeit für manuelle Dateneingaben, spart Administrationszeit und verbessert die Genauigkeit.

DirX Access stellt folgende weitere Administrationsanwendungen zur Verfügung:

- DirX Access Console, eine kommandozeilenorientierte Anwendung auf Basis der Open Services Gateway initiative (OSGi) Shell, die das Einrichten von DirX Access Komponenten und das Verwalten der Policy- und Konfigurationsdaten unterstützt.
- Policy Manager: eine Java Swing Anwendung mit grafischer Benutzerschnittstelle zum Bearbeiten von XACML-Policies und zur Nutzung der DirX Access Policy- und Autorisierungs-Web-Services.

Mandantenfähigkeit

Zur Unterstützung von Mandantenfähigkeit können mehrere Instanzen von DirX Access eingesetzt werden. Jede Instanz repräsentiert einen Mandanten mit einer eigenen, separaten Konfiguration für jeden Mandanten. Dies ermöglicht es, mehrere Kundenorganisationen (Mandanten) mit einer einzigen Installation der Software zu bedienen. DirX Access stellt Mittel zur Verfügung, um zusätzliche Instanzen / Mandanten zu erzeugen.

Audit

Um die Einhaltung von behördlichen und geschäftsinternen Vorschriften und Regelungen nachweisen zu können, stellt DirX Access eine vollständige Übersicht über seine durchgeführten Transaktionen zur Verfügung. Das System:

- auditiert Transaktionen sowohl innerhalb von Security-Domänen als auch über Security-Domänen hinweg
- zeichnet die sicherheitsrelevanten Ereignisse zum Nachweis der Aktivitäten auf, zum Beispiel die Ergebnisse von Authentifizierungs- oder Autorisierungsanfragen oder Passwort- oder Policy-Änderungen.

Alle Autorisierungsanfragen für eine gegebene Transaktion können mit dem zugehörigen, vorhergehenden Authentifizierungsereignis in Beziehung gebracht werden, so dass alle Transaktionen bis zu ihrem Ursprung zurückverfolgt werden können. Dies gilt für alle relevanten Funktionen (Autorisierung, Authentifizierung, Identity Federation, Benutzerverwaltung, Policy- und Konfigurationsverwaltung).

DirX Access generiert Audit-Daten, die direkt mit den Aktionen der authentifizierten Benutzer korrespondieren. Zu den Aktionen, die für jeden Benutzer protokolliert werden, gehören:

- Authentifizierung: wer, wann, wie
- Autorisierung: wer, wann, für was
- Session-Management: Session-Dauer, Idle-Timeout, etc.
- Account- und Passwort-Management: Änderungen, Ablaufdatum erreicht, etc.
- Policy-Management: Anlegen, Ändern, etc. von Rollen, Authentifizierungs- und Autorisierungspolicies
- Benutzerverwaltung: Anlegen, Ändern, etc. von Benutzern und Gruppen
- Konfigurations-Ereignisse

DirX Access stellt eine Schnittstelle zur Audit-Externalisierung zur Verfügung, die kundenspezifische Implementierungen zur Verarbeitung von Audit-Daten über Plugins ermöglicht. Die folgenden Implementierungen werden mit dem Produkt zur Verfügung gestellt:

- Eine auf Log4J basierende Implementierung, die Log4J Appender (zum Beispiel für Konsole, File, Datenbank, Syslog, etc.) zur Verarbeitung von DirX Access Auditereignissen nutzt. Dies ist das Standard-Audit-Plugin, das von DirX Access zur Verfügung gestellt wird.
- Mit DirX Access wird standardmäßig die Integration zum Produkt DirX Audit zur Verfügung gestellt.

DirX Audit kann für die zentrale, sichere Speicherung, die Analyse, die Korrelation und das Review Identitäts-bezogener Audit-Daten sowie zur Erstellung von Reports genutzt werden. DirX Audit gehört ebenfalls zur DirX-Produktfamilie und kann separat bestellt werden.

DirX Access kann seine Konfigurations-, Policy- und Benutzerdaten mittels Web Services in Form von XML-Dateien exportieren. Diese Dateien können mittels XSLT zu kundenspezifischen Reports umgewandelt werden.

Logging

Das DirX Access Logging zeichnet die internen Operationen auf, um Probleme diagnostizieren zu können und Fehler suchen und beseitigen zu können. Die Menge der Informationen, die jeder Server erzeugt, kann gesteuert werden, indem die Aufzeichnungen auf ein bestimmtes Level beschränkt werden.

System Monitoring

Die DirX Access Services und Web Application Container unterstützen das Monitoring mittels Java MBeans. MBeans sind eine Standardmethode im Java-Umfeld zur Überwachung eines Software-Systems. MBeans werden durch die Java Management Extensions (JMX) Technologie unterstützt.

Die DirX Access MBeans stellen sowohl Live-Daten über den Status der Container als auch Nutzungsstatistiken zur Verfügung wie unter anderem

- Anzahl der Authentifizierungsanfragen
- Anzahl der Autorisierungsanfragen
- Anzahl der Anfragen zur Ausstellung von SAML-Assertions

Nagios-Unterstützung

Die von den DirX Access Komponenten unterstützten MBeans können durch eine Reihe von Monitoring-Tools und –Systemen genutzt werden. Speziell ermöglicht DirX Access auch die Integration mit dem weit verbreiteten Monitoring-System Nagios mittels der Drittanbieter-Tools JNRPE, check_nrpe und check_JMX. Diese stellen die Mittel zur Überwachung von Java-Prozessen mittels MBeans zur Verfügung.

Integration und Customization Framework

Die Funktionen und Komponenten von DirX Access sind speziell für die Integration in Kundenumgebungen entworfen worden, so wie in den vorhergehenden Abschnitten beschrieben.

Umfangreiche Konfigurationsmöglichkeiten stellen vielfältige Optionen zur kundenspezifischen Anpassung zur Verfügung, sodass eine einfache Anpassung an Kundenszenarien ermöglicht wird.

DirX Access Architektur

Viele Business-Applikationen können DirX Access für das Access Management und dessen Durchsetzung nutzen, zum Beispiel Portale, Web Server, Application Server, etc. Sie können in vier Schichten unterschieden werden: die Client-, Web-, Applikations- und die Daten-Schicht. DirX Access integriert sich typischerweise in die Web- und Applikationsschicht. Abhängig von den in diesen Schichten eingesetzten Integrationstechnologien können die Standardmöglichkeiten von DirX Access genutzt werden (PEPs, Explorer und Federation Endpunkte), um die Business-Applikationen zu integrieren, oder das DirX Access Client SDK, um weitere Applikationen wie zum Beispiel Legacy-Applikationen zu integrieren.

DirX Access integriert mit den Applikationen, die es schützt, mittels Agenten (sogenannter PEPs – Policy Enforcment Points), die als Plugins zu Web Servern oder Web Application Servern oder anderen Applikationen eingesetzt werden. Sie fungieren als Clients zum DirX Access Server, mit dem Sie den Authentifizierungs- und Autorisierungsprozess durchführen. Sie setzen die Zugriffsentscheidungen des Servers durch und stellen dem Browser des Benutzers und

den nachgelagerten Applikationen Session- und Zustandsinformationen zur Verfügung. Dies schließt auch Reverse Proxy Konfigurationen ein.

Der DirX Access Server stellt die Sicherheitsservices wie Authentifizierung, Autorisierung (PDP Policy Decision Point), SSO, Federation, Policy, Konfiguration für die PEPs zur Verfügung, wickelt den Zugriff zu den LDAP-Datenhaltungen ab, stellt die Services als Web Services und/oder Federation Services für Dritte bereit und stellt die Logik für die Web-basierten Administrationsschnittstellen zur Verfügung.

Die Zugriffsentscheidungen des PDP werden auf Basis von XACML-basierten Autorisierungspolicies getroffen, die vom PAP (Policy Administration Point) verwaltet werden. Der PAP ist durch den Policy-Service im Server implementiert und wird auch als Web Service zur Verfügung gestellt. Der PAP kann über die Web-basierte, grafische Benutzeroberfläche der Administrationskonsole von DirX Access genutzt werden (speziell für RBAC) als auch mit dem DirX Access Policy Manager (speziell für ABAC).

Die PIPs (Policy Information Points) werden eingesetzt, um auf weitere Informationen zuzugreifen, die von der Anfrage betroffen sind, wie Informationen über das Anwendungsumfeld, das Subjekt oder die Ressource.

DirX Access nutzt LDAP Directory Server als Datenhaltung für Benutzer-, Konfigurations- und Policy-Daten.

Die DirX-Architektur kann wie folgt in Schichten strukturiert werden:

- Client-Schicht:
  - DirX Access PEPs und Explorer
  - DirX Access Applikationen wie Federation-Endpunkte, Authentication Application, DirX Access Manager und die Web Services
- Server-Schicht: DirX Access Server, der die Security-Services zur Verfügung stellt
- Daten-Schicht: Directory-Server, die zur Datenhaltung für die Benutzer-, Konfigurations- und Policy-Daten für DirX Access genutzt werden.

Die DirX Access Services und Applikationen werden in einsatzbereiten OSGI-basierten Containern bereitgestellt. Dies ermöglicht die Netzwerktrennung, wobei die Services in einem geschützten Netzwerk und die Applikationen in der DMZ eingesetzt werden können.

Die Abbildung 7 stellt auf hoher Ebene die DirX Access Architektur und ihre Integrationspunkte in existierende Applikationen dar.

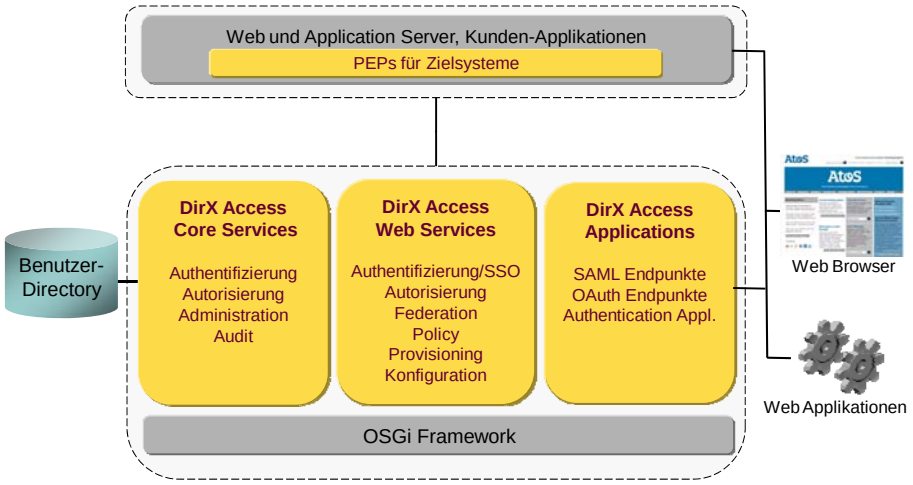

Abb. 7 DirX Access - Architektur und Integration in Anwendungen

Client-Schicht: DirX Access Policy Enforcement Points und Explorer

Policy Enforcement Points (PEPs) sind Plug-in Komponenten, die als DirX Access Clients arbeiten. Sie stellen Services zur Durchsetzung der Policies zur Verfügung (speziell Authentifizierung und Autorisierung). Dafür verarbeiten sie Anfragen nach Ressourcen und Services, fragen den DirX Access Server nach Authentifizierungs- und Autorisierungsentscheidungen ab und stellen diese Entscheidungen zur weiteren Verarbeitung zur Verfügung.

Resource Explorer sind optionale Komponenten, die die Erstellung von Policies unterstützen (siehe Beschreibung unter Administration).

Für Integrationszwecke unterstützt DirX Access auch die Konfiguration beliebiger LDAP-User-Objekte, die über den HTTP-Header der zu sichernden Applikation zur weiteren Nutzung zur Verfügung gestellt werden.

Client-Schicht: DirX Access Applikationen

DirX Access stellt die beiden folgenden Kategorien von Standard-Web-Applikationen zur Verfügung: DirX Access Manager, DirX Access Authentication Application und Federation-Applikationen.

DirX Access Manager stellt ein intuitiv zu bedienendes, Web-basiertes User Interface zur Verfügung, mit dem normale und delegierte Administratoren das System verwalten können (zu den Details siehe den Abschnitt Administration in diesem Dokument).

Die DirX Access Authentication Application ist eine DirX Access Komponente, die die initiale Benutzerauthentifizierung im Auftrag der DirX Access PEP und FEP Komponenten durchführt. Das Layout der Benutzerschnittstelle ist kundenspezifisch anpassbar. Die Authentication Application unterstützt die kontextabhängige Authentifizierung auf Basis der Unterscheidung interner bzw. externer IP-Adressen, wodurch Sicherheitsrisiken minimiert werden können.

Die DirX Access Federation-Applikationen stellen Endpunkte für das föderierte Identity Management zur Verfügung:

- SAML Service Provider Federation Endpunkt (SP FEP), der einen Federation-Endpunkt für SAML Service Provider zur Verfügung stellt
- SAML Identity Provider Federation Endpunkt (IdP FEP), der einen Federation-Endpunkt für SAML Identity Provider zur Verfügung stellt.
- Der SAML Identity Provider Federation Endpunkt unterstützt SuisseID und der SAML Service Provider Federation Endpunkt kann SuisseID-fähige Identity Provider unterstützen. SuisseID ist ein nationales ID-Infrastrukturprojekt in der Schweiz, das einen benutzerzentrischen Identity Management Ansatz unterstützt und die SAML V2.0 Spezifikation durch entsprechende Eigenschaften erweitert.
- Der OAuth Server Federation Endpunkt repräsentiert die Authorization Server Seite der OAuth-Kommunikation. Der Authorization Endpunkt wird vom Client genutzt, um die Autorisierung vom Ressourcen-Eigentümer zu erhalten. Der Token Endpunkt wird vom Client genutzt, um das Authorization Grant gegen das Access Token auszutauschen, typischerweise verbunden mit einer Client-Authentifizierung.
- Der OAuth Client Federation Endpunkt repräsentiert die Client Seite der OAuth-Kommunikation. Er ermöglicht das Erzeugen einer Session in DirX Access. Der OAuth 2.0 Client Federation Endpunkt kann mit OAuth 2.0 Servern zusammenarbeiten, wie zum Beispiel Google, Facebook, etc.

DirX Access Web Services

DirX Access stellt standardmäßig folgende Web Services zur Verfügung:

- Authentifizierungs- und SSO Web Service
- Autorisierungs-Web Service
- Policy Web Service
- Federation Web Service
- Provisioning Web Service
- Konfigurations-Web Service

Einzelheiten siehe im Abschnitt Security Web Services in diesem Dokument.

Server-Schicht: DirX Access Core Services

Die DirX Access Core Services stellen die Kernfunktionalität des Produkts zur Verfügung inklusive Services für Authentifizierung und SSO, Autorisierung, Administration und Audit. Sie sind nach SOA-Prinzipien realisiert und bestehen neben den oben genannten Services aus einer Reihe von weiteren unterstützenden Services.

Die Core Services des DirX Access Servers werden über eigene Schnittstellen als auch über die Web-Applikationen und Web-Services genutzt.

Diese Architektur ermöglicht eine verteilte und sichere Installation der DirX Access Komponenten:

- Die Komponenten der Server-Schicht sind in einem Services Container gebündelt und können in einem geschützten Netzwerk installiert und mit einer zusätzlichen Firewall geschützt werden.
- Die Komponenten der Client-Schicht sind in einem Web Applications Container gebündelt und können zusammen mit den Web Servern mit den DirX Access PEPs in einer DMZ installiert und mit einer zusätzlichen Firewall geschützt werden.

Daten-Schicht: Directory Server

DirX Access kann zwei unterschiedliche LDAP Directory Server parallel nutzen, einen für die Benutzerdaten und einen für die Policy-/ Konfigurationsdaten.

Jedes standardkonforme LDAP Directory mit einem Schema, das für die Benutzerverwaltung geeignet ist (zum Beispiel mit der InetOrgPerson Objektklasse), kann als Benutzerdatenhaltung dienen.

DirX Access kann die Benutzerdaten, die es vom Benutzerdirectory erhält, mit Informationen aus anderen Datenhaltungen ergänzen. Dazu können sowohl Standard- und/oder kundenspezifisch entwickelte Attribut Finder genutzt werden, die funktional mit virtuellen Directories vergleichbar sind.

Die Policy-Daten in der Datenhaltung umfassen die folgenden Elemente:

- Authentifizierungs-Policies
- Autorisierungspolicies (RBAC/ABAC) inklusive Regeln, Bedingungen und Aktionen

Die Konfigurationsdaten in der Datenhaltung umfassen die folgenden Elemente:

- Authentifizierungsmethoden
- die Server-Konfiguration
- die Konfigurationsdaten der Policy Enforcement Points
- die Konfigurationsdaten für die Federation-Endpunkte
- die Konfigurationsparameter für die zentralen Komponenten wie Angaben zur Benutzerdatenhaltung, Templates für SAML Assertions, etc.

Applikationen zur Benutzerverwaltung können mit dem DirX Access Server über die Provisioningschnittstellle angebunden werden.

Ebenso kann DirX Access verschiedene LDAP-Directory-Server nutzen. Diese sind nicht Teil der Produktlieferung von DirX Access.

Ausfallsicherheit, Hochverfügbarkeit und Skalierbarkeit

Um die höchstmögliche Verfügbarkeit, Ausfallsicherheit und Skalierbarkeit zu erreichen, kann DirX Access redundant installiert werden. Mehrere DirX Access Server können konfiguriert werden. Die DirX Access Clients wie PEPs oder Federation-Endpunkte können die Last beim Zugriff auf die DirX Access Server verteilen. Dazu halten die DirX Access Clients einen internen Verbindungs-Pool und einen Health-Index der verschiedenen, aktuell verfügbaren Server. Die Lastverteilung erfolgt dann auf Basis dieses Verbindungs-Pools. Um die Ausfallsicherheit des Systems zu ergänzen, unterstützen die DirX Access Server Master-/Shadow-Konfigurationen des Directory-Systems.

DirX Access nutzt eine Reihe ausgeklügelter Mechanismen, um beim Ausfall von Systemkomponenten wieder aufzusetzen und um Ausfallzeiten für die Benutzer zu vermeiden, inklusive

- eines verteilten Cache, der es den DirX Access Servern erlaubt, die Security-Objekte und Konfigurationsdaten gemeinsam zu nutzen
- Lastverteilung zwischen DirX Access Servern basierend auf dem Round-Robin Algorithmus
- Wiederanlauf der Operationen basierend auf Wiederholungsversuchen in festgelegten Intervallen und Fehlerschwellwerten

Verhalten der Clients

Jede Applikation, die innerhalb des Systems als DirX Access Client arbeitet, muss einen zugehörigen Eintrag in der DirX Access Konfigurationsdatenhaltung haben. Wenn ein DirX Access Client die Kommunikation mit dem DirX Access Server startet, muss er einen Instanzennamen zur Verfügung stellen. Der Konfigurations-Service nutzt diesen Instanzennamen, um den dazugehörigen Konfigurationseintrag in der Konfigurationsdatenhaltung zu finden. Dieser umfasst die Adressen aller DirX Access Server in einem Cluster oder eine ausgewählte Untermenge dieser Server, die diesem Client zugeordnet sind, zusammen mit weiteren Informationen wie zum Beispiel die maximale Anzahl von Verbindungen, die der Client starten darf.

Wenn eine Applikation Anfragen an die DirX Access Server sendet, verteilen die zugrundeliegenden DirX Access Clients die Last transparent auf die konfigurierten DirX Access Server. Zudem werden automatisch die Serververbindungen erzeugt, die benötigt werden, um den Nachrichtenaustausch zu bearbeiten, bis hin zum festgelegten Maximum. Wenn dieser Schwellwert erreicht ist, arbeitet der DirX Access Client seine Nachrichten mit den verfügbaren Verbindungen und Servern ab.

Gemeinsame Nutzung der Session-Zustände

Mehrere DirX Access Server in einem Netzwerk nutzen einen synchronisierten Cache, der die Session-Objekte, die Policies und die Konfigurationsattribute enthält. Dieser Cache ermöglicht es Clients (PEPs, FEPs), Anfragen zu beliebigen Servern in einem Netzwerk zu senden und verbessert die Leistung, da die Anzahl der Leseanfragen zum Directory Server reduziert wird.

Zusätzlich verbessert der Cache die Möglichkeiten zur Ausfallsicherheit, da ein Session-Objekt, das von einem Server erzeugt und im Cache gespeichert wird, von einem anderen Server wieder genutzt werden kann. Wann immer ein Server ausfällt, können die anderen Server die Session transparent fortführen, ohne die Sicherheit der Transaktion zu beeinträchtigen.

Jedes Mal, wenn ein Benutzer erfolgreich authentifiziert wird, wird eine neue Session initiiert, die ein neues Subjekt im Cache anlegt. Das Subjekt enthält den Session Token zusammen mit der Liste von Attributen (z.B. die Rollenzuweisungen) des authentifizierten Benutzers sowie weitere Informationen. Da der Cache verteilt ist, sind die Session-Zustände sofort für alle anderen Server verfügbar. Zwischen den DirX Access Servern gibt es kein Konzept für eine Objekteigentümerschaft. Wenn, aus welchem Grund auch immer, ein Server runterfährt oder nicht mehr verfügbar ist, wird die Last transparent auf die restlichen Server verteilt.

LDAP-Failover

Der Zugriff auf die Konfigurations- und Policy-Datenhaltung im LDAP-Directory-Server ist äußerst wichtig und wird sichergestellt, indem auf einen zweiten Directory-Server umgeschaltet wird, falls der erste nicht mehr verfügbar ist. Wenn der DirX Access Server als Antwort auf eine Directory-Operation ein Timeout erhält, wird er versuchen, stattdessen den zweiten Directory-Server zu benutzen.

Unterstützte Standards

DirX Access unterstützt die relevanten Standards, Protokolle und Security Frameworks bei seinen Sicherheitsfunktionen und –services.

Für Autorisierung und Vertraulichkeit unterstützt DirX Access XACML V1.x/2.0/3.0, XACML 3.0 Multiple Decision Profile Version 1.0, XACML SAML Profile Version 2.0, SAML V1.x/V2.0, OAuth 2.0 und RBAC.

DirX Access hat im Jahr 2009 die Interoperabilitätstests der Liberty Alliance bestanden, als es am dritten Liberty Interoperable™ Full-Matrix Test-Event für SAML V2.0 teilgenommen hat.

Für die initiale Benutzerauthentifizierung in Web-Umgebungen unterstützt DirX Access SSL/TLS, HTTP Basic Authentication, HTML Form-based Authentication mit Username/Passwort, One-Time-Passwörter basierend auf den IETF RFCs 2289, 4226 und 6238 und FIDO U2F.

Für Single Sign-On innerhalb einer Domäne in Web-Umgebungen unterstützt DirX Access Integrated Windows Authentication (SPNEGO/Kerberos, NTLM), authentifizierte Subjekt-Identifier, die mittels HTTP Cookie Header übertragen werden und URL Rewriting.

Für Single Sign-On zwischen verschiedenen Domänen und Identity Federation in Web-Umgebungen unterstützt DirX Access SAML V1.x/V2.0 speziell SAML Web-SSO Profile und WS-Federation Passive Requestor Profile Version 1.0.

Für Single Sign-On zwischen verschiedenen Domänen und Identity Federation in Web-Services-Umgebungen unterstützt DirX Access WS-Trust.

Die Implementierung des OAuth 2.0 Authorization Frameworks zusammen mit den nachfolgend genannten Erweiterungen ermöglicht, dass DirX Access in nahezu jedem plausiblen Federation-Szenario eingesetzt werden kann:

- The OAuth 2.0 Authorization Framework (RFC6749)
- The OAuth 2.0 Authorization Framework: Bearer Token (RFC6750)
- OAuth 2.0 Authorization Server Metadata, https://tools.ietf.org/html/draft-ietf-oauth-discovery-06
- OpenID Connect 1.0
- OpenID Connect Discovery 1.0
- OAuth 2.0 Token Revocation (RFC7009)
- OAuth 2.0 Token Introspection (RFC7662)
- OAuth 2.0 Dynamic Client Registration Protocol (RFC7591)
- OpenID Connect Dynamic Client Registration Protocol
- OAuth 2.0 Resource Registration
- Federated Authorization for User-Managed Access 2.0
- User-Managed Access 2.0 Grant for OAuth 2.0 Authorization

Für die sichere Kommunikation unterstützt DirX Access SSL/TLS and WS-* Security.

Zum Schützen von Objekten unterstützt DirX Access XML Signature.

Für das Key-Management unterstützt DirX Access PKCS und X.509/PKIX.

Für die Kommunikation unterstützt DirX Access HTTP, SOAP, und WS-*.

Für die persistente Datenhaltung und für die Provisionierung unterstützt DirX Access LDAP, DSML und SPML.

In Java-Umgebungen unterstützt DirX Access JAAS, JACC, JCA/JCE, JGSS, und JSSE.

DirX Access unterstützt Internet Protocol IPv4 und IPv6.

Weitere DirX Produkte

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

DirX Directory stellt einen standardkonformen, leistungsstarken, hochverfügbaren, sehr zuverlässigen und sicheren LDAP und X.500 Directory Server und LDAP Proxy 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 risikobasierte 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 Audit Auditoren, Sicherheitsbeauftragten und Administratoren analytischen Einblick und Transparenz in Identity und Access Management Prozesse. Mit 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 auf Identitätsdaten, ein grafisches Dashboard, einen Monitor für Identitäts-bezogene 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.

Technische Voraussetzungen für DirX Access V8.7

Unterstützte Plattformen für Policy Enforcement Points, Resource Explorer und Client SDK:

Die folgende Tabelle zeigt die unterstützten Kombinationen auf. Weitere PEPs können auf Anfrage verfügbar sein.

	Microsoft Windows Server 2012 R2 / 2016	Red Hat Enterprise Linux 7	SUSE Linux Enterprise Server 12
Web Server PEPs			
Apache httpd V2.4	Ja	Ja	Ja
Reverse Proxy (basierend auf Apache httpd V2.4)	Ja	Ja	Ja
Apache Tomcat V7.0/8.0	Ja	Ja	Ja
Eclipse Jetty 8	Ja	Ja	Ja
Microsoft IIS	Ja	-	-
Servlet und Applikationsspezifische PEPs			
Servlet Filter z.B. Tomcat, Jetty, etc.	Ja	Ja	Ja
Cloud Foundry	[1] -	-[1]	-[1]
Client SDK Unterstützung (Legacy Applikationen PEPs und Explorer)			
DirX Access Client SDK für Java 1.6 oder höher	Ja	Ja	Ja

[1] Der Cloud Foundry PEP kann in einer existierenden Cloud Foundry Provider Umgebung eingesetzt werden.

Technische Voraussetzungen für DirX Access V8.7

Hardware

- Intel Server Plattform für Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Linux

Speicheranforderungen

Hauptspeicher:	mindestens 4 GB
Plattenspeicher:	mindestens 1 GB plus Plattenspeicher für Daten

Software

DirX Access Server

Der DirX Access Server als Java-Anwendung wird auf folgenden Plattformen unterstützt, wobei für die gewählte Plattform die aktuellsten Patches/Service Packs erforderlich sind:

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

- Java SE Runtime Environment (JRE) 8 für das gewählte Betriebssystem

Unterstützung virtueller Maschinen:

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

Unterstützte LDAP-Directories für Konfigurations-/Policy-Daten

DirX Access unterstützt die folgenden LDAP-Directories (weitere auf Anfrage):

- DirX Directory V8.4/V8.5/V8.6
- Microsoft Windows Server 2012 R2/2016 Active Directory / Active Directory Lightweight Directory Services (AD LDS)

Unterstützte LDAP-Directories für Benutzerdaten

Beliebige LDAPv3-konforme Directory Server mit Benutzerdaten basierend auf der InetOrgPerson Objektklasse

Unterstützte Browser für DirX Access Manager und Deployment Manager

- Microsoft Internet Explorer 11
- Microsoft Edge
- Firefox 52 oder neuer
- Google Chrome 62 oder neuer

Für die Nagios-Integration

- Nagios Core Version 4.0.8
- JNRPE Server, Version 2.0.5
- JNRPE Plugins, Version 2.0.3

Unterstützte PEPs, Explorer und Application Server:

Diese Komponenten sind auf der vorherigen Seite aufgeführt.

Benutzeroberfläche

Englisch

Dokumentation

Folgende Manuale werden in englischer Sprache bereitgestellt:

- Release Notes
- Installation Guide
- Administration Guide
- Integration Guide
- Client SDK Documentation (JavaDoc)

www.evidian.com