EVIDEN

Identity und Access Management

DirX Access V9.1

Vertrauensvolle Zusammenarbeit

Identity Federation, SSO und Access Management 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 aus, die nicht zum Kerngeschäft gehören, und bieten ihren Nutzern vielfältige 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.

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 (SaaS) 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 über- lasten oder versehentlich Sicherheitslücken zu erzeugen.

Um die Benutzerzufriedenheit zu maximieren, muss eine sichere, nahtlose Transaktion zwischen Diensten unterschiedlicher Sites in unter- schiedlichen 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.

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 Federation und 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 Sicherheitsrichtlinien 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.

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

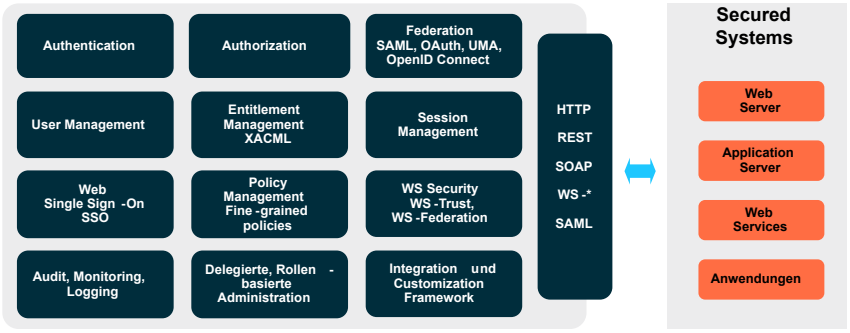

Abbildung 1 - DirX Access Funktionalität

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 zu- gehörigen 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, FIDO basierte Authentifizierung, integrierte Windows-Authentifizierung, Smartcards, HTML Forms, One-Time Password (OTP) und Biometrie. Mittels eines Interface‘ können weitere Authentisierungsmethoden wie z.B. mobile push integriert werden. 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 Anmeldedaten merken, und die Administratoren müssen nicht länger redundante Authentifizierungsmechanismen unterstützen.

Jede Aktion, die ein Benutzer in einem von DirX Access geschützten System durchführt, beginnt mit einer initialen Authentifizierung. Nachfolgende Aktionen nutzen das Single-Sign-On Verfahren. Die risikobasierte Authentifizierung wird in beiden Fällen angewendet, um vom Benutzer zusätzliche und stärkere Authentifizierungen an zu fordern. Die Weiterleitung des Authentifizierungs-Status an andere verbundene Systeme erfolgt mittels Identity Federation.

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 oder HTML Form Authentifizierung mittels Username/Passwort
- OTP mobile push Verfahren, die einen zusätzlichen Kanal nutzen, wie SMS und Email basierende Authentifizierung über HTML Form.
- Standard-basierte OTP Verfahren IETF RFC 4226 (HOTP) und IETF RFC 6238 (TOTP) via HTML form
- Integrierte Windows-Authentifizierung (IWA) mittels SPNEGO, Kerberos und NTLM Protokoll (via http)
- W3C Web Authentication basierend auf FIDO2 inklusive Authentifizierung mit Microsoft Windows Hello
- FIDO U2F (Universal 2nd Factor)
- FIDO UAF (Universal Authentication Framework)

DirX Access unterstützt bei der Verbesserung des Authentifizierungs-Prozesses durch 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. Die Kombination und Sequenz von verschiedenen Verfahren kann konfiguriert und an Bedingungen geknüpft werden.

Z.B. ein Fehler in der ersten Methode, kann den Zugang sperren oder zu einer anderen Authentifizierung auffordern. Damit kann DirX Access ausgefeilte Verfahren zur Verfügung stellen, die das Sperren von Accounts verhindern. Nach drei erfolglosen Versuchen mit Benutzername und Passwort, wird der Benutzer aufgefordert sich mit seinem X.509 Zertifikat zu authentifizieren, um das Sperren des Accounts und eine möglicherweise teure Entsperrung zu verhindern.

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 verschiedene Algorithmen, eine Schnittstelle für Verifizierungsverfahren anderer Hersteller unterstützt Authentifizierung mittels Tokens, 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 authentifiziert 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 Anmeldedaten und andere Parameter, die dem Login-Ereignis zuzuordnen sind. DirX Access stellt eine Schnitt- stelle 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 wer- den, zum Beispiel von lösungsspezifischen Sicherheitsumgebungen wie Informationen zum Trust-Level des Netzwerks oder zur Art des Gerätes, das genutzt wird.

DirX Access erzeugt für jede initiale Authentifizierung eine neue Security-Session. Eine Security-Session wird eingerichtet zwischen Webbrowsern und einem DirX Access Server mit eigenständigen JSON Web Token (JWT), kombiniert mit Verweisen auf den Internen verteilten Cache. Dieser Ansatz erreicht die besten Ergebnisse in Bezug auf Leistung und Hochverfügbarkeitsfunktionen. Je nach Sicherheitsstufe kann das Token (JWT) nicht nur digital signiert, sondern auch verschlüsselt werden (ist somit vollständig vertrauenwürdig).

Eine bestehende Security-Session wird beendet durch ein explizites Logout (ausgelöst durch den Benutzer), nach Session Timeout oder nach Idle Timeout. Dank der Verwendung des in sich geschlossenen-Sitzungstoken (JWT), wird die Sitzungen nicht durch einen Neustart des gesamten DirX Zugriffsserver-Cluster beendet.

Zu den weiteren Session-Management Eigenschaften von DirX Access gehören:

- 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.

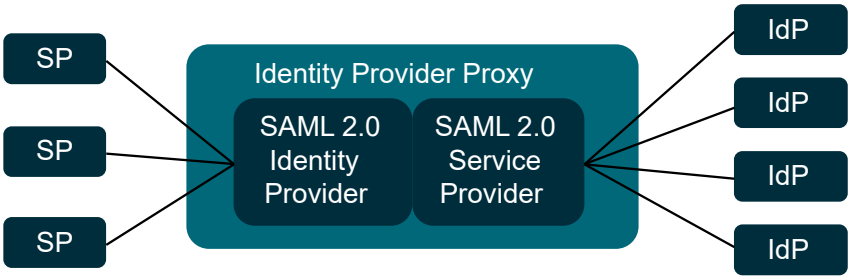

Abbildung 2 - DirX Access - SAML Proxying IdP

Identity Federation und föderierte Authentifizierung

Identity Federation ist eine 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, WS-Federation als auch via OpenID Connect 1.0.

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. 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, NameIds 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 AssertionConsumer- Service 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/oder mehreren Service Providern konfiguriert werden, so dass der Proxying IdP als Drehscheibe (Hub, Bridge, Gateway) in einem Identity Federation Verbund eingesetzt werden kann.

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.

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

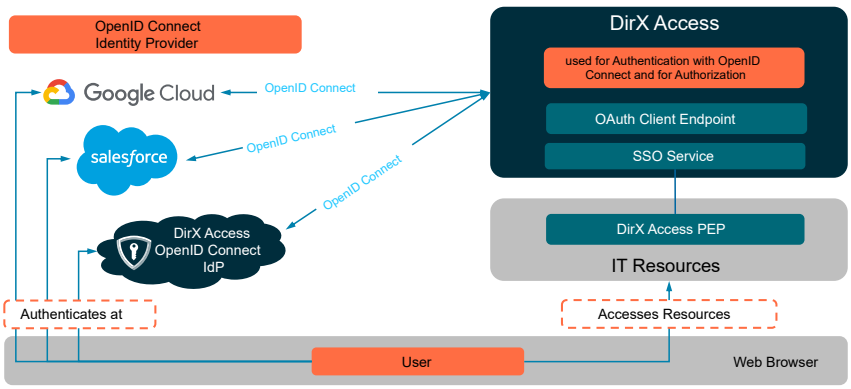

Abbildung 3 - SSO mit sozialen Identitäten basierend auf OpenID Connect

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.

Auf Basis der OpenID Connect Standards unterstützt DirX Access zusätzlich das OpenID Connect Dynamic Registration Protocol und OpenID Connect Discovery 1.0.

OpenID Connect ist zu einer etablierten Alternative des SAML Protokolls geworden, da es von allen wesentlichen Service Providern wie Google, Facbook, etc unterstützt wird. Basierend auf einfacheren Technologien (RESTful Web Services und JSON Format) sind OpenID Connect und OAuth in der Lage, die Anforderungen an die Netzperformance zu reduzieren und dennoch die Sicherheit der anderen Federation Standards zu erhalten.

OpenID Connect 1.0 Autorisierungs Prozess

Mit OpenID Connect 1.0, kann ein Client (Web Application) eine federated Identity eines Benutzers von einem Autorisierungs-Server (repräsentiert durch DirX Access) anfordern. Der Benutzer hat die Möglichkeit für die Übertragung seiner Identity Informationen sein Einverständnis zu erklären.

OpenID Connect 1.0 Implicit Flow

Im Gegensatz zum Autorisierungs-Prozess benötigt der OpenID Connect Implicit Prozess keine Client Authentifizierung. Die Information über die Federated Identity könnte z.B. für jeden sichtbar sein, der Zugriff auf den Browser des Benutzers hat. Diese Form ist für Client Implementierungen, die auf Script-Sprachen von Browsern basieren vorgesehen.

OpenID Connect Dynamic Client Registrierung

In Umgebungen, in denen Web Applicationen (Clients) sehr oft Federated Identity Informationen unterschiedlichster Art benötigen und damit z.B. mehr als 100mal angefragt werden, kann die Verbindung zum Autorisierungs-Server kompliziert werden. Diese Verbindungen werden vom Client und Server durch sogenannte Metadaten Dokumente dargestellt. DirX Access publiziert die Metadaten von allen konfigurierten Autorisierungs-Servern in standardisierter Form damit alle potentiellen Clients darauf zugreifen können. In umgekehrter Richtung wird die dynamische Client Registrierung verwendet, um die Registrierung von neuen Clients zu automatisieren oder Metadaten von registrierten Clients zu aktualisieren. Die Metadaten können manuell vom DirX Access Administrator verwaltet werden, um Client Spezifika abzubilden.

Um einen möglichst hohe Automatisierungsgrad zu erreichen, stellt DirX Access eine feingranulare Konfiguration für die Client Registrierung zur Verfügung. Am Ende des Registrierungs-Prozesses wird für den Client ein bestimmtes Zugriffsrecht eingestellt, z.B. welche Identity Informationen abgefragt werden können, welche Prozesse dürfen ausgeführt werden, oder welche Sicherheitsstandards muss der Client befolgen. Durch die Delegation von Vertrauen wird sichergestellt, dass nur vertrauenswürdige Clients Informationen abfragen können. Bevor ein Client sich registrieren kann, muss eine Authentifizierung stattfinden. Die Authentifizierung kann von jeder Entität durchgeführt werden, die bei DirX Access registriert ist und für die das Recht vergeben wurde, später weitere Clients zu registrieren. Ein Administrator kann das Recht bekommen, automatisch Clients mit bestimmten Rechten zu registrieren.

Das beschriebene Metadaten-Management wird für alle OAuth basierten Standards durchgeführt.

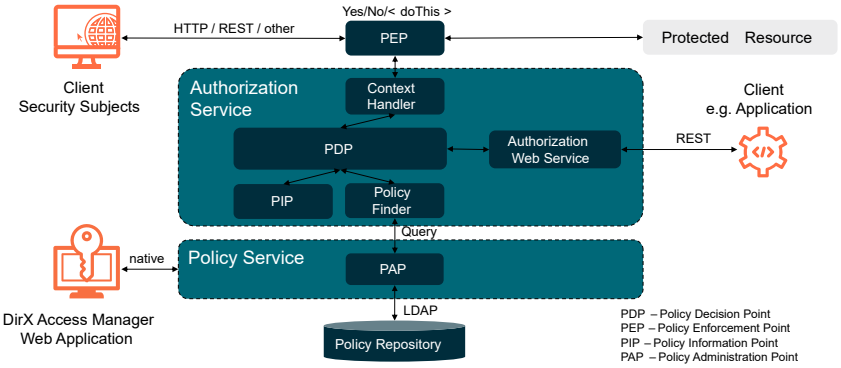

Abbildung 4 - DirX Access – XACML-basiertes Autorisierungssystem

DirX Access as OpenID Connect 1.0 Client

Die Abbildung 3 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.

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.

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 und OpenID Connect genutzt.

Inter-protocol Proxying

Dank seiner Architektur kann DirX Access eine Proxy Funktion zwischen unterschiedlichen Identity Federation Protokollen wie SAML und OAuth zur Verfügung stellen. Wenn ein SAML Service Provider (SAML SP) Informationen von einem SAML Identity Provider (SAML IdP) wird entweder eine Authentifizierung des Benutzers oder der SSO Prozess durchgeführt. Jede Authentisierungsmethode kann dabei genutzt werden. Während der Authentifizierung wechselt DirX Access seine Rolle vom SAML IdP / OIDC AS zum SAML SP / OIDC Client.

Autorisierung und Entitlement Management

DirX Access stellt zwei grundsätzlich unterschiedliche Autorisierungsverfahren zur Verfügung. Für Enterprise und Organisationen wird Autorisierung als externer, zentraler, Policy-basierter Access Service zur Verfügung gestellt. Dieser erlaubt es umfassende Access Policies zu definieren und anzuwenden. Dieses Verfahren wird durch die XACML Autorisierungs-Standards beschrieben.

Mit dem Aufkommen von IoT, inkludiert DirX Access auch Standards, die Ressourcen schützen, die Dritten gehören. Im Gegensatz zum zentralen Policy-basiertem Ansatz, deklariert jeder Eigentümer einer Ressource seine Policy selbst. während DirX Access den nachgelagerten Autorisierungs-Vorgang durchführt. Dieses Verfahren basiert auf den UMA 2.0 Standards (User Managed Access).

Beide Ansätze sind unabhängig voneinander und können von DirX Access konfiguriert und angewendet werden, abhängig vom gewählten Lösungsansatz.

Enterprise Autorisierung

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

Zum Beispiel werden beim Rollenbasierten Zugriffskontrollmodell (RBAC, Role-Based Access Control) die Access Policies basierend auf den Rollen der Benutzer festgelegt, während bei der Attribut-basierten Zugriffskontrolle (ABAC, Attribute-Based Access Control) die Access Policies basierend auf Attributwerten der Benutzer festgelegt werden und bei der Zugriffskontrolle nach Ermessen (DAC, Discretionary Access Control), die Access Policies 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 Access Policies erfolgt unabhängig von der einzelnen Applikation und die Notwendigkeit für die Implementierung einer Zugriffskontrolllogik für jede einzelne Applikation kann vermieden werden. Die Erzeugung von Access Control Policies 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. Mitarbeitern können Rollen zugewiesen werden, die ihrem Arbeitsauftrag und Ressourcenbedarf entsprechen. Wenn entsprechende Business-Rollen in DirX Access definiert wurden, können Administratoren sehr einfach Rechte zuweisen, ohne zu befürchten, für den Zugriff wichtige Ressourcen zu vergessen. Dieses Autorisierungsmodell wird auf Basis des RBAC-Profils von XACML formuliert, das heißt, dass die Policies, die in diesem Autorisierungsmodell formuliert werden können, die Anforderungen dieses speziellen Profils erfüllen müssen.

Innerhalb von DirX Access wird die Autorisierung von folgenden Komponenten bereitgestellt (siehe Abbildung 4):

- 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 Autorisierungs-Policies, die sie von PAPs erhalten.
- PAPs (Policy Administration Points) sind Autorisierungs-Policy-Instanzen, die es den Administratoren ermöglichen, Autorisierungs-Policies 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 Autorisierungs-Policies), 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) und OAuth 2.0 Dynamic Client Registration Protocol (RFC 7591). Eine Liste der unterstützen Standards befindet sich am Ende des Dokuments.

OAuth 2.0

DirX Access unterstützt den OAuth 2.0 Authorization Framework für die Autorisierung in Federation Szenarien. OAuth definiert ein Ressourcenbezogenes 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 Browserbasiertem 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)

Der Fokus bei der Autorisierung in einer IoT Umgebung (in der Regel viele Ressource Eigentümer) wird mit DirX Access durch den Standard UMA 2.0 realisiert. Dieser Standard ermöglicht es, die Komplexität des Autorisierungsmanagement zu delegieren (z.B. Verwaltung von medizinischen Daten, bring your own device, oder upload von Benutzer Ressourcen, etc. DirX Access ist in diesem Szenario der Autorisierungs-Server (AS) und das angeschlossene System ist der Ressource-Service (RS). Es stellt über ein RESTful Interface dem Ressource Eigentümer die Möglichkeit zur Verfügung, um die Ressourcen-bezogenen Policies zu deklarieren (typischerweise in Form einer Access Control List), welche später vom AS ausgewertet werden, wenn eine geschützte Ressource angefordert wird. Das bedeutet, dass die gesamte Last auf den AS verlagert wird, während der RS nur Information über den Ressource-Identifier haben muss.

Die Mächtigkeit des AS liegt in der Fähigkeit, die Ressourcen von vielen RS zu verwalten. Die Beziehung von RS und AS wird durch OAuth Mittel zur Verfügung gestellt, während DirX Access zusätzlich die Automatisierung des Vorgangs übernimmt und damit bestens für aaS-Umgebungen geeignet ist.

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 Authori- zation und Ressource Server in einem Res- sourcen-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.

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 Autorisierungs-Policies, etc.) genutzt werden. Dazu können Daten aus beliebigen LDAP-Verzeichnissen herangezogen werden.

DirX Access implementiert den SCIM 2.0 Standard und erweitert die Basisstruktur, um die Ressourcen für spezielle Datentypen für die Authentisierung, wie z.B. OTP shared Secrets oder FIDO credentials, etc.

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 Autorisierungs-Policies 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.

Authentifizierungs-Polices setzen die Anwendung von spezifischen Authentifizierungsmethoden für die jeweilige Ressource durch.

Autorisierungs-Policies wenden Autorisierungsregeln an, die die Zugriffe auf geschützte Ressourcen steuern. Feingranulare Autorisierungs-Policies 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.

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 zwei unterschiedliche Web Services Technologien zur Verfügung: RESTful und SOAP WS. Die RESTful WS wurden entsprechend dem Open Data Protocol (OData) Version 4.0 Standard der OASIS implementiert. Das Interface wurde mittels OpenAPI 3 Format beschreiben, so dass es sehr einfach in Anwendungen integriert werden kann.

DirX Access stellt standardmäßig die folgenden Web-Services zur Verfügung:

- SSO Web Service: ein zentraler Zugangspunkt für alle notwendigen Funktionen zur Bewertung einer Anfrage: Authentifizierung (initial, step-up, risikobasiert), Autorisierung, SSO, Anfrage-/Antwort-Injektion
- Federation Web Service: ein Web-Service, 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.
- Die Systemaktionen-Web-Services: ermöglichen die Bereitstel-

lung von Komponenten, für die Keystore-Verwaltung, usw.

Administration

Administrationszuständigkeiten im Unternehmen spiegeln oftmals die Geschäftsstruktur wider, 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 Zugriffs-Policies schnell und effizient in der Organisation zum Einsatz gebracht werden 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 5). Die Administratoren können mit dem DirX Access Manager eine Reihe von Aufgaben ausführen wie:

- Erzeugen von Business-Rollen
- Erzeugen von Authentifizierungs-Policies 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
- Konfiguration der XACML Policies

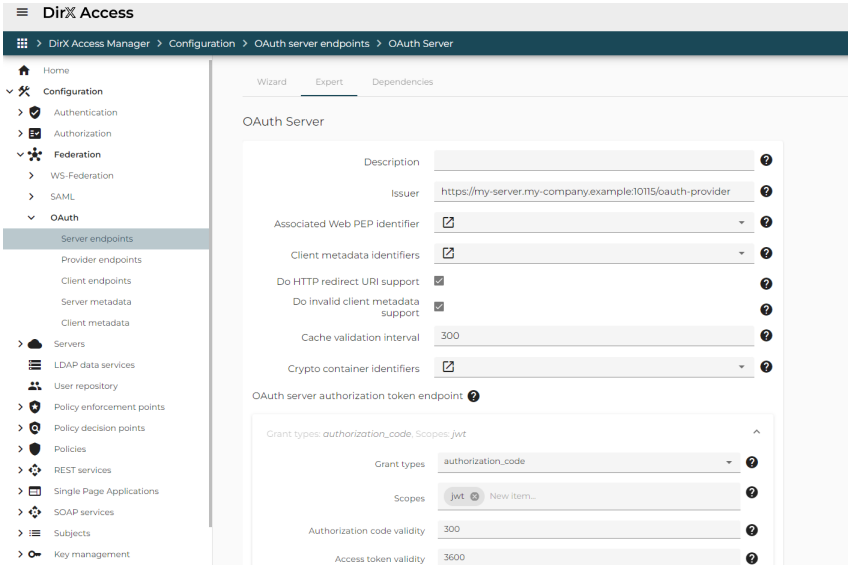

Abbildung 5 - DirX Access Manager Beispiel der Administrationsoberfläche

- 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

Der DirX Access Manager ist eine Single-Page Webanwendung, die RESTful-Schnittstellen verwendet, welche vom DirX Access Server bereitgestellt werden. Diese sind der SysActions RESTful Web-Service, der die Bereitstellung jeder DXA-Komponente oder Webanwendung ermöglicht, und der Configuration RESTful Web-Service, der die Verwaltung von Konfiguration und Richtlinien ermöglicht.

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

- 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 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

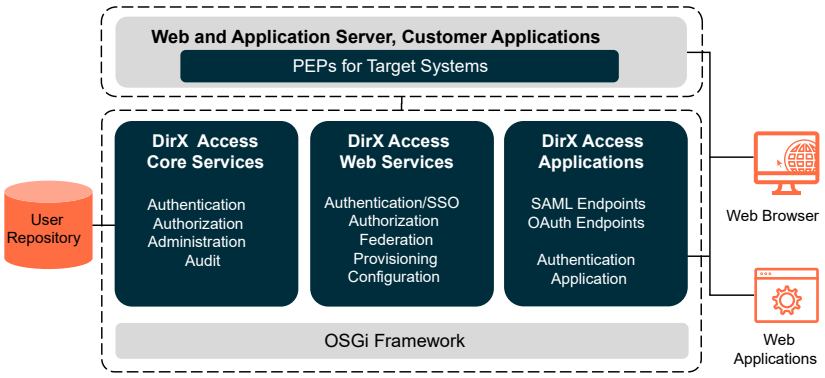

Abbildung 6 - DirX Access - Architektur und Integration in Anwendungen

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.

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 und Federation Endpunkte), um die Business-Applikationen zu integrieren.

DirX Access integriert mit den Applikationen, die es schützt, mittels Standard Federation Protocol oder 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.

Die PIPs (Policy Information Points) werden eingesetzt, um auf weitere Informationen wie Informationen über das Anwendungsumfeld, das Subjekt oder die Ressource.

DirX Access verwendet LDAP-Verzeichnisdienste zum Speichern von Benutzer-, Konfigurations- und Richtliniendaten, außerdem den DirX Access Cache Server zur Vereinfachung der verteilten Natur des Systems, mit dem Fokus auf Daten-Caching und Daten-Persistenz.

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

Client-Schicht:

- DirX Access PEPs

Server-Schicht:

- DirX Access Server, der die Security-Services zur Verfügung stellt
- DirX Access Applikationen wie Federation-Endpunkte, Authentication Application, DirX Access Manager und die Web-Services

Datenschicht:

- Verzeichnisdienste zum Speichern von Benutzer-, Konfigurations- und Richtliniendaten für den DirX Access Cache Server zum Cachen und Persistenz der verteilten Systeminformationen, z. B. erweiterte SSO-Informationen, langlebige Federation-Daten usw.

Die DirX Access Services und Applikationen werden in einsatzbereiten OSGI-basierten Containern bereitgestellt.

Die Abbildung 6 stellt auf hoher Ebene die DirX Access Architektur und ihre Integrationspunkte in existierende Applikationen dar.

Client-Schicht: DirX Access Policy Enforcement Points

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.

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.

Server-Schicht: DirX Access Applikationen

DirX Access stellt die 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 sowie die Abfolge der Authentisierungen sind 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. Ein Benutzer Informationsendpunkt wird vom Client genutzt, um einen Access Tokens über Identity Daten der authentifizierten Entität auszutauschen. Die Metadaten und der Client Registirierungs-Endpunkt werden für Metadaten Austausch und Registrierung genutzt. Während die Policy Management Endpunkte zuständig sind für die Verwaltung der Policies für Ressourcen, die vom Ressource-Eigentümer im connected System gespeichert sind (UMA 2.0 Autorisierungs-Prozess),
- 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:

- SSO Web Service
- Authentifizierungs Web-Service
- Autorisierungs-Web-Service
- Federation-Web-Service
- Provisioning-Web-Service
- Konfigurations-Web-Service
- Systemaktionen-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.

Daten-Schicht: Directory Server

DirX Access kann zwei unterschiedliche LDAP Directory Server parallel nutzen, einen für die Benutzerdaten und einen für die DirX Access spezifischen Policy- und 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
- Autorisierungs-Policies (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.

Ein LDAP Directory Server wird nicht nur für die Speicherung der Konfigurations-Daten, sondern auch für die von DirX Access generierten benutzerspezifischen Daten genutzt, wie z.B. RBAC Daten, verschiedene Anmeldedaten, FIDO- bezogene Daten, OTP Anmeldedaten, etc.

Wenn entsprechende Methoden für den Benutzer konfiguriert sind. Speichert der Directory Server alle zugröhrigen Benutzerdaten.

Applikationen zur Benutzerverwaltung können mit dem DirX Access Server über die Provisioning-Schnittstelle angebunden werden.

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

Datenschicht: DirX Access Cache Server

DirX Access Server kann eine beliebige Anzahl von DirX Access Cache Servern verwenden, um verteiltes Caching und Persistenz zu ermöglichen. Dies ist überwiegend notwendig, um folgende Funktionen zu unterstützen:

- Erweiterte SSO-Session-Informationen (z.B. eingehende SAML-Zusicherungen gebunden an die Sitzung),
- Langlebige OAuth-Tokens (z. B. Refresh-Token)
- Verteilung von Informationen zwischen Servern (z. B. verteiltes einmaliges Abmelden in SAML)

Das empfohlene Deployment sieht einen DirX Access Cache Server in Verbdinung mit einem DirX Access Server vor. Dies hängt jedoch komplett von den benötigten Hochverfügbarkeitsfunktionen ab.

In einer instabilen und dynamischen Umgebung kann der DirX Access Server kurzfristig auch ohne den DirX Access Cache Server arbeiten, sollte dieser ausfallen, und dennoch die am häufigsten verwendeten Funktionen (wie z.B. SSO, initial Authentifizierung usw.) bereitstellen.

Ausfallsicherheit, Hochverfügbarkeit und Skalierbarkeit

Um die höchstmögliche Verfügbarkeit, Ausfallsicherheit und Skalierbarkeit zu erreichen, können DirX Access Server (und entsprechende DirX Access Cache Server) redundant installiert werden. Mehrere DirX Access Server können konfiguriert werden. Die DirX Access Clients wie PEPs 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

- Verteilter Cache und Persistenz, basierend auf DirX Access Cache Server-Komponenten. Der verteilte Cache und die Persistenz ermöglichen es dem DirX Access Server, sicherheitsrelevante Objekte zu teilen und persistent 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 Instanz-Namen, 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.

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.

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 4226

und 6238 und FIDO U2F, UAF, W3C WebAuthentication (basiert auf dem FIDO2 Eingaben).

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 Ver- sion 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-dis- covery-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 Proto- col (RFC7591)
- OpenID Connect Dynamic Client Registration Protocol
- OAuth 2.0 Resource Registration
- Proof Key zum Code-Austausch (RFC7636)
- 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 und WS-* Security.

Für benutzerspezifische Provisionierung unterstützt DirX Access SCIM 2.0.

Zum Schützen von Objekten unterstützt DirX Access XML Signaturen.

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.

Technische Voraussetzungen

Unterstützte Plattformen für Policy Enforcement Points und Client SDK:

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

	Microsoft Windows Server 2019 / 2022	Red Hat Enterprise Linux 7 / 8	SUSE Linux Enterprise Server 12 / 15
Web Server PEPs			
Apache httpd V2.4 [2)]	Ja	Ja	Ja
Reverse Proxy (basierend auf Apache httpd V2.4)	Ja	Ja	Ja
Apache Tomcat V8.5/9.0/10.0	Ja	Ja	Ja
Eclipse Jetty 8/9/10/11	Ja	Ja	Ja
Microsoft IIS [2)]	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)			
DirX Access Client SDK für Java 8 oder höher	Ja	Ja	Ja

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

[2)] PEPs sind nicht Lieferumfang enthalten und stehen auf Anfrage zur Verfügung oder per Service Pack.

Technische Voraussetzungen

Hardware

- Intel Server-Plattform für Microsoft Windows Server 2019 und 2022
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server

Speicherbedarf:

Hauptspeicher: mindestens 8 GB

Plattenspeicher: mindestens 1 GB plus Speicher für Daten

Software

DirX Access Server

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

- Microsoft Windows Server 2019 (x86-64)
- Microsoft Windows Server 2022 (x86-64)
- Red Hat Enterprise Linux 7 (x86-64)
- Red Hat Enterprise Linux 8 (x86-64)
- SUSE Linux Enterprise Server 12 (x86-64)
- SUSE Linux Enterprise Server 15 (x86-64)
- Java SE Runtime Environment (JRE) 11 für das gewählte Betriebssystem

Unterstützung virtueller Maschinen:

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

Unterstützte LDAP-Directories für Konfigurations-/Policy-Daten

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

- DirX Directory V8.9/V8.10
- Microsoft Windows Server 2019/2022 Active Directory / Active Directory Lightweight Directory Services (AD LDS)

Unterstützte LDAP-Directories für Benutzerdaten

- Beliebige LDAPv3-konforme Directory Server mit Benutzerdaten basierend auf der Inet-Org-Person Objektklasse

Unterstützte Browser für DirX Access Manager und Deployment Manager

- Microsoft Internet Explorer 11
- Microsoft Edge
- Firefox 71 oder neuer
- Google Chrome 78 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 und Application Server

Diese Komponenten sind auf der vorherigen Seite aufgeführt.

Benutzeroberfläche

- Englisch

Dokumentation

- Folgende Manuale werden in Englisch bereitgestellt:

Manuale

- Release Notes
- Introduction Guide
- Installation Guide
- Administration Guide
- Integration Guide

DirX Produkt-Suite

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

DirX Identity

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, Risiko-basierte 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, Zugriffszertifizierungen, Passwortmanagement, Metadirectory sowie Audit- und Report-Funktionalität.

DirX Directory

DirX Directory bietet einen standardkonformen, hochperformanten, hochverfügbaren, hochzuverlässigen, hochskalierbaren und sicheren LDAP- und X.500-Directory-Server und LDAP-Proxy mit sehr hoher linearer Skalierbarkeit. DirX Directory kann als Identitätsspeicher für Mitarbeiter, Kunden, Partner, Abonnenten und andere IoT-Einheiten dienen. Es kann auch als Bereitstellungs-, Zugriffsverwaltungs- und Metaverzeichnis-Repository dienen, um einen einzigen Zugriffspunkt auf die Informationen in unterschiedlichen und heterogenen Verzeichnissen bereitzustellen, die in einem Unternehmensnetzwerk oder einer Cloud-Umgebung für die Benutzerverwaltung und -bereitstellung verfügbar sind.

DirX Access

DirX Access ist eine umfassende, Cloud-fähige, skalierbare und hochverfügbare Zugriffsverwaltungslösung, die richtlinien- und risikobasierte Authentifizierung, Autorisierung basierend auf XACML und Föderation für Webanwendungen und -dienste bietet. DirX Access bietet Single Sign-On, vielseitige Authentifizierung einschließlich FIDO, Identitätsföderation basierend auf SAML, OAuth und OpenID Connect, Just-in-Time-Bereitstellung, Berechtigungsverwaltung und Richtliniendurchsetzung für Anwendungen und Dienste in der Cloud oder vor Ort.

DirX Audit

DirX Audit bietet Auditoren, Security-Compliance-Beauftragten und Audit-Administratoren analytische Einblicke und Transparenz für Identität und Zugriff. Basierend auf historischen Identitätsdaten und aufgezeichneten Ereignissen aus den Identitäts- und Zugriffsverwaltungsprozessen ermöglicht DirX Audit die Beantwortung der „Was, Wann, Wo, Wer und Warum"-Fragen zu Benutzerzugriff und Berechtigungen. DirX Audit bietet historische Ansichten und Berichte zu Identitätsdaten, ein grafisches Dashboard mit Drilldown zu einzelnen Ereignissen, einen Monitor zum Filtern, Analysieren, Korrelieren und Überprüfen von identitätsbezogenen Ereignissen und eine Auftragsverwaltung für die Berichterstellung. Mit seinen analytischen Funktionen unterstützt DirX Audit Unternehmen und Organisationen dabei, eine nachhaltige Compliance sicherzustellen und Business Intelligence für die risikobasierten Identity- und Access-Management-Prozesse bereitzustellen.

Connect with us

eviden.com