EVIDEN

Identity und Access Management

DirX Directory 9.1

High-End Directory Server

Standardkonformer, leistungsstarker, hochverfügbarer, skalierbarer und sicherer LDAP / X.500 Directory Server und LDAP Proxy

Directory Server sind wesentliche Komponenten in der heutigen vernetzten e-Business-Landschaft, in der sie die Basis für das Identity und Access Management sowohl für das Unternehmen intern als auch über die Unternehmensgrenzen hinaus bilden. Für das Intranet stellt der Directory Service eine globale Datenhaltung für gemeinsam benutzte Informationen über Mitarbeiter, Organisationen sowie Ressourcen wie Applikationen, Netzwerkkomponenten, IoT Devices und andere verteilte Dienste zur Verfügung, wobei ein Directory Server Daten von mehreren Hunderttausend Benutzern aufnehmen muss. In Extranet-Umgebungen verwaltet der Directory Server Informationen über Kunden, Partner und Lieferanten, wobei Daten von mehreren Millionen Nutzern zu verwalten sind. Für beide genannten Einsatzumgebungen muss der Directory Server Informationen über Benutzeridentitäten verwalten, den Zugriff zu diesen Informationen kontrollieren sowie schnellen, hochverfügbaren und authentifizierten Zugriff zu den Informationen für eine möglicherweise sehr große Anzahl von Benutzern zur Verfügung stellen.

DirX Directory erfüllt sowohl die oben genannten als auch wichtige weitere Anforderungen. Der DirX Directory Server stellt eine standardkonforme, leistungsstarke, hochverfügbare, sehr zuverlässige und sichere Identity Management Plattform mit sehr hoher linearer Skalierbarkeit zur Verfügung.

DirX Directory kann als Identity-Datenhaltung für Informationen über Mitarbeiter, Kunden, Geschäftspartner, Abonnenten von Diensten, IoT Devices sowie über andere Teilnehmer von e-Business-Verfahren dienen.

Ebenso kann DirX Directory auch als Datenhaltung für das Provisioning, Access Management und Metadirectory dienen, die zentrale Zugriffsschnittstelle zu Informationen aus verschiedenen heterogenen Directories, die in einem Unternehmen oder in Cloud-Umgebungen für die Benutzerverwaltung und das Provisioning eingesetzt wird.

Standards und Kompatibilität

DirX Directory unterstützt die LDAPv3 und X.500 Standards. DirX Directory ermöglicht die Schemaverwaltung über LDAP. DirX Directory läuft auf den gängigen Betriebssystemplattformen und unterstützt eine Vielzahl von Directory-Anwendungen über die LDAP-Schnittstelle.

Der DirX Directory LDAP-Proxy stellt einen zentralen Zugangspunkts für alle angeschlossenen LDAP-Clients zur Verfügung, so dass diese nicht wissen müssen, welcher konkrete LDAP-Server die Anfragen verarbeitet, eventuelle Ausfälle von Ziel-Servern nicht auf die Clients rückwirken und Lastverteilung transparent für die Clients erfolgt.

Hohe Performance

DirX Directory basiert auf dem innovativen, für den Directory-Zugriff optimierten DBAM-Datenbankkern (Directory Basic Access Method) und bietet damit schnelle Antwortzeiten und hohe Durchsatzraten für parallele Anfragen. DBAM bietet einen hochleistungsfähigen Datenbank-Cache für Pufferung von Teilen der Directory-Daten im Hauptspeicher (in Memory Datenbank).

Hohe Verfügbarkeit und Zuverlässigkeit

Um die Anforderungen hinsichtlich der Zuverlässigkeit eines Directory Service zu erfüllen, unterstützt DirX Directory die Floating Master Replikation für Hochverfügbarkeitskonfigurationen und Ausfallsicherung, d.h. eine Software-Lösung anstelle des Einsatzes von Hardware-Clustern. Beim Backup bzw. Recovery unterstützt DirX Directory Voll- und Differenzsicherungen, auch parallel zu Schreiboperationen. Transaktionsunterstützung in der Datenbank ermöglicht die Wiederherstellung nach Systemausfällen ohne Datenverlust.

Identity Management

Als Basis für ein Identity Management System ermöglicht DirX Directory die Verwaltung von Benutzer- und Teilnehmerprofilen, digitalen Zertifikaten für Public Key Infrastrukturen, Autorisierungs- und Authentifizierungsinformationen, Zugangsberechtigungen und anderen für Benutzer und Teilnehmer relevanten Attributen, um einen geschützten Zugang zu Daten, Netzwerkressourcen oder verteilten Diensten bereitzustellen.

Sicherheit

DirX Directory unterstützt SSL/TLS für LDAP-Server und Client Authentifizierung, X.500 DAP Authentifizierung, autorisierte Benutzerzugriffskontrolle, verschlüsselte Kommunikation sowie Server-Policies für die lokale Sicherheitsverwaltung. DirX Directory erlaubt die Verwaltung und die Durchsetzung von Passwort Policies, um zu steuern, wie Passwörter

in einem Unternehmensnetzwerk eingesetzt werden. Dabei werden Policies wie Komplexität, Alter oder Wiedernutzbarkeit der Passwörter nach deren Ablauf unterstützt. Für die Analyse des Datenverkehrs und für Abrechnungszwecke steht ein leistungsfähiges Audit Logging zur Verfügung.

Skalierbarkeit

Die DBAM-Datenbank ist für lineare Skalierbarkeit in einem Directory Server konzipiert. Damit wird sowohl zukünftiges Wachstum mit existierenden Hardware-Konfigurationen ermöglicht als auch die Skalierbarkeit von Unternehmens-Directories bis hin zu e-Business-, Extranet- oder Cloud-Directories mit sehr großen Mengen an Benutzerdaten.

Weitere Möglichkeiten zur Konfiguration von Skalierbarkeit und Hochverfügbarkeit stehen mit dem Einsatz des DirX Directory LDAP-Servers im Proxy-Modus zur Verfügung. In diesem Modus wird für angeschlossene LDAP-Clients ein zentraler Zugangspunkt zum Directory Service bereitgestellt.

Administration

DirX Directory bietet leistungsstarke grafische und Kommando-orientierte Administrationswerkzeuge zur zentralen Verwaltung eines verteilten Directory-Systems inklusive Auditing, Monitoring- und Logging-Funktionen.

Zugriff auf DirX Directory

Der Zugriff auf die in DirX Directory gespeicherten Daten ist möglich über

- beliebige LDAP-Clients und LDAP-Anwendungen
- eine Kommando-basierte Administrations-Schnittstelle mit voller LDAP-Funktionalität, die zusätzlich über Tcl-Scripts steuerbar ist
- DirX Manager, den Java-basierten Management Client.
- DirX Corporate Directory, eine Angular-basierte Webanwendung, die die REST-Dienste nutzt

Die Komponenten von DirX Directory

- Directory System Agent DSA
- LDAP-Server und LDAP-Proxy
- Java-basierte, grafische Administrations-Oberfläche DirX Manager zur Konfiguration und Administration von lokalen und entfernten DirX Directory Servern
- Kommando-gesteuerte Tools dirxload und dirxmodify zum schnellen Laden großer Datenmengen (bulkloading)
- Kommando-basierter Directory Client dirxcp zur Administration von Einträgen via LDAP und DAP
- Kommando-gesteuerter Management-Client dirxadm zur Administration der DSA- und LDAP-Server
- Kommando-gesteuertes Tool dirxbackup zum Sichern und Wiederherstellen der Datenbank
- HTTP Server für RESTful API Zugriffe
-

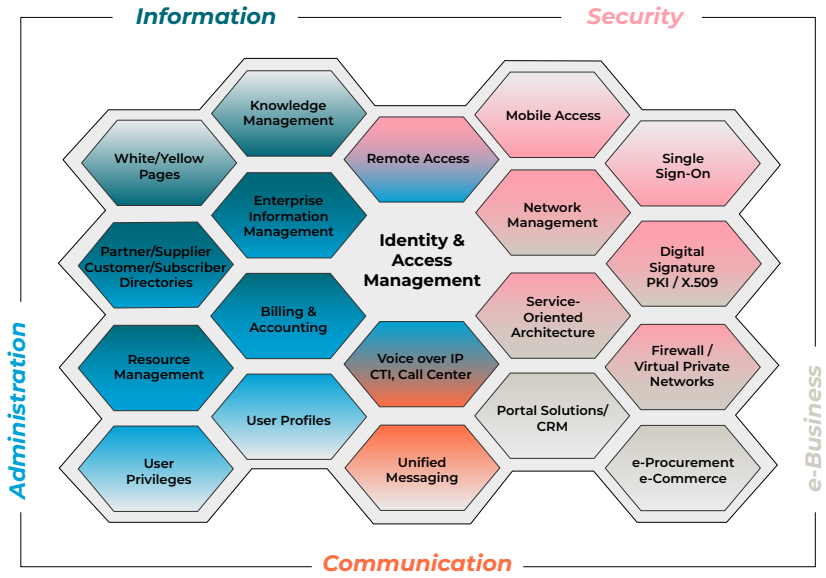

Abbildung 1 - DirX Directory – Anwendungsbereiche

Directory Protokolle

Es werden folgende Protokolle nach den Internet-Standards und den 1993er X.500-Standards unterstützt:

LDAP: Das Lightweight Directory Access Protocol wird durch einen integrierten LDAP-Server effizient unterstützt.

DAP: Das Directory Access Protocol, das den Austausch von Anfragen zwischen Directory User Agents DUA und Directory System Agents DSA definiert.

DSP: Das Directory System Protocol, über das DSAs Anfragen und Verwaltungsaufträge an andere DSAs weiterleiten, die sie selbst nicht beantworten können. Hier wird auch die Rückgabe des Ergebnisses an den DSA behandelt, der die Suchanfrage oder den Auftrag ursprünglich gestellt hat.

DISP: Das Directory Information Shadowing Protocol regelt die Replikation der Daten zwischen DSAs. Da das Protokoll auch das Kopieren der Zugriffskontrolldaten, der kollektiven Attribute und der Schema-Information regelt, kann auf die replizierten Daten ohne Informationsverlust zugegriffen werden.

IDM: Das Internet Directly Mapped Protocol (IDM) bildet die X.500-Protokolle direkt auf TCP/IP ab und wird für DAP, DSP und DISP unterstützt.

X.500 Informations-Modell

DirX Directory ist konform zum Informationsmodell des 1993er X.500 Standards und unterstützt u.a.

- Collective Attributes - identische Attribute mehrerer Directory-Einträge, auf die wie auf normale Attribute zugegriffen wird, die aber nur ein einziges Mal zentral gespeichert und administriert werden
- Zugriffskontrollregeln für Teile eines Directory-Baums
- Attribut Subtyping, die Möglichkeit des Zugriffs auf spezifische Attribute durch Referenzieren generischer Attribute (zum Beispiel privateTelephoneNumber als Subtyp von telephoneNumber)
- Operative Attribute – Attribute, die für interne Zwecke benutzt werden oder die, wie zum Beispiel Zeitstempel, vom Directory selbst generiert werden.

Directory Schema

DirX Directory unterstützt die Attribut-Typen und Syntaxen, die gemäß X.520 definiert sind. Zusätz-

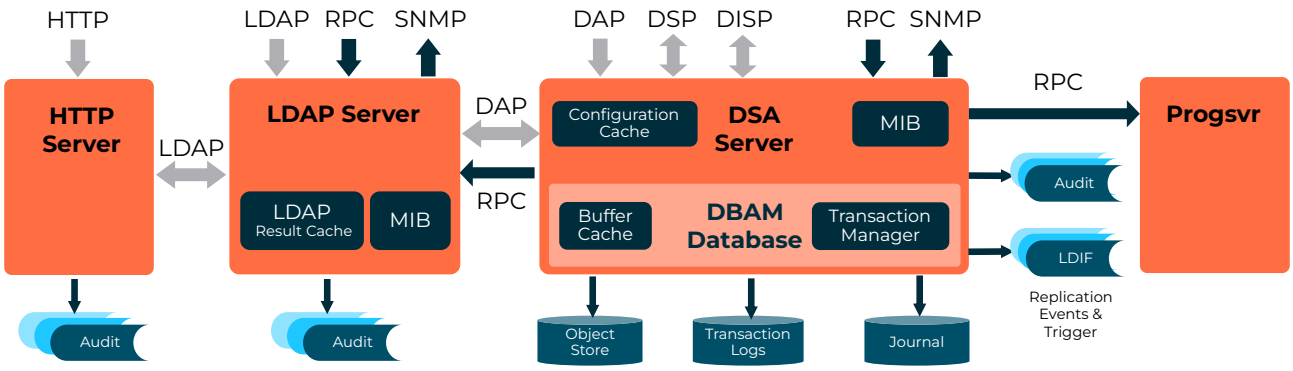

Abbildung 2 - DirX Directory - Architektur

lich werden die in X.509 definierten Attributtypen sowie die in X.521 definierten Vergleichsregeln (matching rules) unterstützt. Unterstützt werden auch phonetische Regeln zum Auffinden von Einträgen mit ähnlichen Werten.

Ebenso werden alle in X.521 definierten Objektklassen unterstützt sowie alle Objektklassen, Attributtypen und Syntaxen gemäß den LDAP-RFCs 4512, 4517, 4523 und 2798 (inetOrgPerson).

DirX Directory ermöglicht die Speicherung von X.509 Attributzertifikaten basierend auf der Unterstützung von X.509(2000)-Attributzertifikat-Syntaxen.

DirX Directory unterstützt das ACP 133 Schema gemäß dem Dokument „Common Directory Services and Procedures Supplement ACP 133 SUPP-1(A)" vom Combined Communications Electronics Board (CCEB).

Als Erweiterung zu den X.500 Standards und LDAP RFCs unterstützt DirX Directory dynamische sowie mehrstufig verschachtelte Gruppen. Um LDAP-Applikationen bei der Identifizierung und Auflösung von Mitgliedschaften in dynamischen und verschachtelten Gruppen zu unterstützen, stehen diverse Attribute zur Verfügung. DirX Directory ermöglicht die Nutzung sowohl von dynamischen als auch von verschachtelten Gruppen bei der Verwaltung von Zugriffskontroll- und User-Policies.

Der LDAP-Server unterstützt die Attribute der LDAP Root DSE nach RFC3045 und RFC4512.

DirX Directory unterstützt das Schema Management über Standard LDAPv3 Clients wie DirX Manager oder mit dem Tool dirxmodify. Es erlaubt sowohl die Administration von Standard Schema-Elementen als auch die Definition und Verwaltung von privaten Objektklassen und Attributen.

DirX Directory ermöglicht es, die Eindeutigkeit von Attributwerten für bestimmte Attributtypen (mit String-Syntax) innerhalb eines Directory Servers und all seiner vollen Shadows durchzusetzen.

LDAP-Server

DirX Directory enthält einen LDAPv3 Server, der den Zugriff von beliebigen LDAP Clients erlaubt. Der LDAP-Server implementiert die grundlegenden LDAPv3 Protokolle.

Der LDAP-Server kann auf dem gleichen Rechner wie der DSA oder auf einem entfernten System installiert werden.

Zur Lastverteilung der Zugriffe können mehrere LDAP-Server mit einem DSA verbunden werden oder ein LDAP-Server kann mit mehreren DSAs verbunden werden, falls diese vollständige Shadow-Server sind. In diesem Fall können LDAP Clients auch von den vorhandenen Failover-Möglichkeiten profitieren, da in den meisten Fällen Client-Operationen auch dann noch erfolgreich durchgeführt werden können, wenn einer der verbundenen DSAs ausfällt.

Der LDAP-Server unterstützt die sichere Kommunikation mittels SSL/TLS.

Der LDAP-Server enthält einen konfigurierbaren, hochleistungsfähigen Result Cache, der selektiv aktualisiert werden kann. Damit ist DirX Directory für hochperformante Anwendungen geeignet.

Wenn der DirX Directory LDAP-Server im Proxy-Modus eingesetzt wird, leitet dieser, als LDAP-Proxy, eingehende LDAPv3-Anfragen von LDAP-Clients zu einem entfernten Ziel LDAPv3 Directory Server weiter und liefert die zugehörigen Antworten an den anfragenden Client zurück.

Der wesentliche Vorteil eines LDAP-Proxys ist die Bereitstellung eines zentralen Zugangspunkts für alle angeschlossenen LDAP-Clients, so dass diese nicht wissen müssen, welcher konkrete LDAP-Server die Anfragen verarbeitet, eventuelle Ausfälle von Ziel-Servern nicht auf die Clients rückwirken und Lastverteilung transparent für die Clients erfolgt.

DBAM Datenverwaltung

Die Datenhaltung bzw. -verwaltung von DirX Directory baut auf dem innovativen DBAM Datenbankkern auf, der eine hocheffiziente Basis für extrem hohe Skalierbarkeit, einen optimalen Zugriff und die Modellierung des Directory-Baums bietet.

Zu den wichtigsten Vorteilen der Datenbank gehören

- Sehr hohe Speicherkapazität
- Optimale Indexierung für schnelle und effiziente Suchvorgänge
- hochleistungsfähige Namensauflösung und -suche
- hochleistungsfähiger Datenbank-Cache für Pufferung von Teilen der Directory-Daten im Hauptspeicher
- hochleistungsfähige Transaktions- und Recovery-Unterstützung
- Unterstützung des LDAP RFC 2696 zur Aufbereitung von umfangreichen Ergebnislisten

DirX Directory bietet zur Verwaltung der DBAM- Datenbank Tools für folgende Funktionen an:

- Konfiguration der DBAM-Datenbank
- Überprüfen der DBAM-Datenbank
- Nachindexierung von Attributen

- Reorganisation der Datenbank, für einen optimierten Zugriff
- Sichern und Wiederherstellen der Datenbank

LDIF

DirX Directory unterstützt den hochperformanten Export von LDIF-Dateien (LDAP Data Interchange Format). Über die sogenannten LDIF Content Files kann entweder der gesamte Datenbestand des DirX Directory DSA oder Teile davon exportiert werden. Über die LDIF Change Files können Änderungen der Daten exportiert werden.

Mittels LDIF-Dateien können Administratoren Massendaten von und zur DirX Directory Datenhaltung übertragen und die Daten von anderen Directories integrieren, wobei DirX Directory auch als Datenhaltung für ein Metadirectory genutzt werden kann. LDIF-Dateien bieten die Schnittstelle für Directory Change Events. Die Nachverarbeitung von LDIF-Dateien kann automatisch ausgelöst werden.

Replikation

DirX Directory unterstützt die Erstellung und das automatische Update von Kopien der Directory Daten (Replikation, Shadowing), um die Verfügbarkeit der Daten und die Zugriffsleistung zu erhöhen.

In einem Shadowing-Szenario repliziert ein Master-DSA Daten zu einem oder mehreren Shadow-DSAs. Zur Sicherstellung von Hochverfügbarkeit unterstützt DirX Directory das Floating Master Konzept, bei dem ein Shadow-DSA als neuer Master fungieren kann, wenn beim alten Master-DSA ein Fehler auftritt.

Jeder Shadow DSA kann entweder im synchronen oder asynchronen Shadowing-Modus betrieben werden.

Da die Synchronität der Daten sichergestellt ist, ist ein synchroner Shadow-DSA ein idealer Kandidat für den Einsatz sowohl für Lastverteilungszwecke sowie für das Failover in einem Floating Master Szenario.

Ein synchroner Shadow-DSA ist ebenfalls geeignet für LDAP-/DAP-Clients, die Lese-Operationen unmittelbar nach einer erfolgreichen Änderungsoperation ausführen:

wann auch immer eine LDAP-/DAP-Client-Anwendung nach einer erfolgreichen Änderungsoperation liest, bekommt sie das richtige Ergebnis zurückgeliefert.

Während synchrones Shadowing immer den ganzen Directory-Baum des Masters repliziert, bietet asynchrones Shadowing höhere Flexibilität hinsichtlich der Auswahl der Attribute oder der Teile des Directory-Baums, die repliziert werden sollen.

In DirX Directory stehen folgende Shadowing-Optionen stehen zur Verfügung:

- Differenz-Replikation oder eine Total-Replikation wird über DISP unterstützt
- Periodische Updates und Updates aufgrund von Änderungen werden über DISP unterstützt
- Basierend auf den Save- und Restore-Funktionen der Datenbank wird ein sehr schnelles Replizieren der Daten unterstützt, das zum vollständigen Wiederherstellen der Daten eingesetzt wird.

Verteilung

Skalierbarkeit, Hochverfügbarkeit, Lastverteilung und Performance-Tuning sind die wesentlichen Gründe, um einen verteilten Directory Service aufzubauen. Dazu unterstützt DirX Directory eine Reihe von Optionen:

- Aufbau eines verteilten Directory Service basierend auf Replikation der Daten, wobei ein Master-DSA den vollständigen Directory Information Tree (DIT) hält und Shadow-DSAs Kopien des DIT halten
- Aufbau eines richtigen verteilten Directory Information Tree (DIT), bei dem mehrere DSAs jeweils einen Teil des DITs halten
- Eine Kombination aus Verteilung und Shadowing, bei der Teile des DIT von zwei unterschiedlichen DSAs gehalten werden und jeweils zum anderen DSA repliziert werden
- LDAP- und DSA-Server können auf unterschiedlichen Rechnern eingesetzt werden und mehrere LDAP-Server können mit einem DSA-Server verbunden werden

Die DSAs kommunizieren über DSP, um gegenüber Anwendungen eine einheitliche Sicht des verteilten Directory Service zur Verfügung zu stellen.

Sicherheit

DirX Directory unterstützt SSL/TLS (Secure Socket Layer 3.0 / Transport Layer Security 1.0/1.1/1.2/1.3) und schafft damit die Voraussetzung für die authentifizierte und verschlüsselte Kommunikation über das Internet sowohl für

- LDAP-Server und LDAP-Clients als auch für
- X500 Protokolle DAP, DSP und DISP für die X.500 DSA-zu-DSA- und DUA-zu-DSA-Kommunikation über IDM.

Zusätzlich unterstützt DirX Directory:

- Authentifizierung (Authentication) zwischen DUA und DSA mittels DAP Protokoll oder zwischen Servern mittels Server-Server-Protokollen
- Zugriffskontrolle (Access Control), um den Zugriff auf berechtigte Benutzer einzuschränken
- Verfahren für lokales Sicherheitsmanagement auf der Serverseite.

Authentifizierung

Für die Authentifizierung über LDAP gibt es eine Reihe von Sicherheitsabstufungen, die je nach Anforderung zum Einsatz kommen:

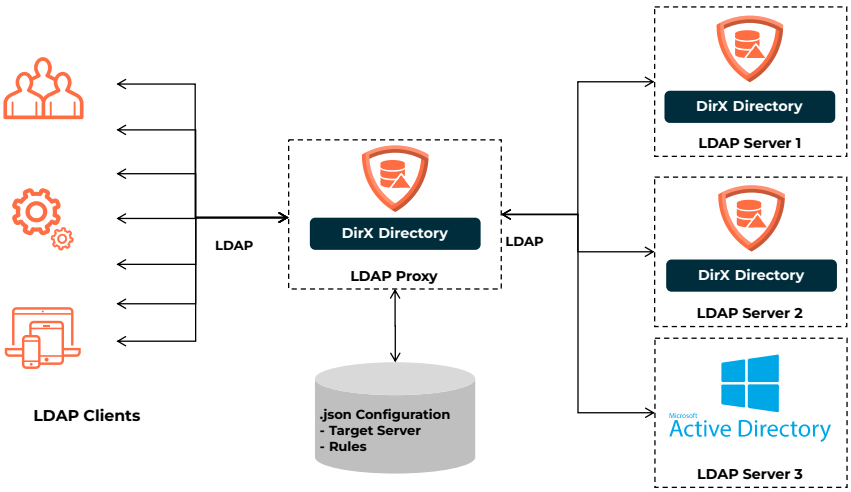

Abbildung 3 - DirX Directory - LDAP Proxy

- Simple Bind mit Name und Passwort
- Simple Bind mit Name und Passwort über eine verschlüsselte SSL/TLS-Verbindung
- SASL Authentication mit Mechanismus EXTERNAL (Zertifikats-basierte SSL/TLS Client Authentication)
- Konfigurierbare Unterstützung für externe Authentifizierung für LDAP Simple Binds über Microsoft Windows oder über LDAPv3, zum Beispiel zu einem IBM RACF LDAP-Server.

DirX Directory unterstützt Certificate Revocation Lists (CRLs), das heißt, dass ein widerrufenes Zertifikat aus einer vorgegebenen CRL nicht mehr genutzt werden kann, um sich erfolgreich mit SASL zu authentifizieren.

DirX Manager unterstützt die Authentifizierung / das Login mittels CardOS-Smartcards auf Basis des Atos CardOS API. Aus Sicht des LDAPv3 Protokolls wird das Smartcard-Login auf einen LDAP-Bind mit dem Mechanismus EXTERNAL abgebildet. Dies bedeutet, dass die Security Services der darunterliegenden TLS/SSL-Schicht genutzt werden, um die Client-Authentication durchzuführen, die auf starker Kryptographie basiert.

Zugriffskontrolle

Der Zugriff auf DirX Directory Informationen ist mehrfach gesichert und bis hin zu einzelnen Attributen innerhalb der Einträge definierbar. DirX Directory unterstützt sowohl die Basic Access Control (BAC) als auch die Simplified Access Control (SAC) inklusive der Access Control Information für Einträge, Sub-Einträge und Attribute.

Als Erweiterung zum X.500-Modell können sowohl die Ziele der Zugriffskontrolle als auch die betroffenen Benutzer durch beliebige LDAP-Filter definiert werden.

Das „Proxied Authorization" Modell wird gemäß RFC 4370 unterstützt.

Zusätzlich bietet die Audit-Funktionalität die Möglichkeit, die Sicherheit des Systems zu überwachen und zu dokumentieren.

Passwort Policies

Zur Verbesserung der Directory-Sicherheit können mit DirX Directory Password Policies festgelegt werden, deren Einhaltung vom System überwacht und durchgesetzt wird. Pass-

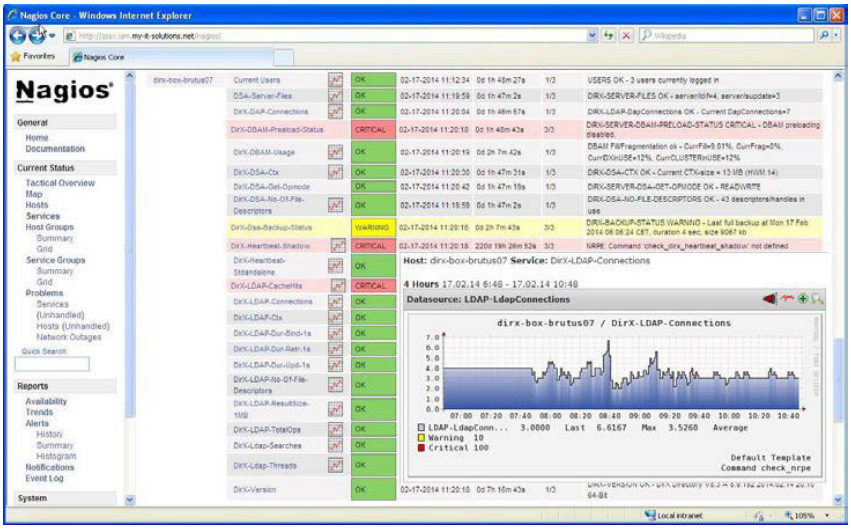

Abbildung 4 - DirX Directory - Nagios Integration Beispiele

word Policies sind eine Menge von Regeln, die steuern, wie Passwörter in einem IT-System benutzt und verwaltet werden. Die Regeln stellen sicher, dass

- Passwörter festgelegten Anforderungen genügen, damit Benutzer nicht einfach zu erratende Passwörter wählen (Password Check Syntax, Password Minimum Length, Password Maximum Length, Password Minimum Special Characters, Password Minimum Lower Case Characters, Password Minimum Upper Case Characters, Password Minimum Numeric Characters, Ausschluss der Nutzung einer Teilzeichenfolge des Namens als Passwort)
- Benutzer ihre Passwörter periodisch ändern (Password Minimum Age, Password Maximum Age, Password Expire Warning, Password Grace Login Limit)
- die Nutzung alter Passwörter eingeschränkt wird (Password In History, Password Must Change)
- Accounts nach fehlerhaften Login-Versuchen gesperrt werden (Password Lockout, Password Lockout Duration, Password Maximum Failure, Password Failure Counter Interval).

Zusätzlich stellen sie Informationen über den Level und Algorithmus für das Password Hashing (Password Storage Scheme, Password Storage Scheme Level) und steuern die operationalen Attribute für den letzten Anmeldezeitpunkt und die Anzahl fehlerhafter Anmeldeversuche.

Unterstützte Password Storage Schemes: unverschlüsselt, hashed, salted-hashed.

Unterstützte Password Storage Hash Algorithmen: SHA-1 und SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512).

Jeder Benutzereintrag enthält eine Reihe von operationalen Attributen, die aktuelle Statusinformationen bereitstellen, um die Verarbeitung der Password Policies zu unterstützen in Bezug auf

- die Passwort-Prüfung
- das Alter des Passworts
- die Sperre des Accounts
- und die Passwort-Verwaltung

Unterstützung von Public Key Infrastrukturen

DirX Directory unterstützt den Standard X.509V3(97) für die sichere Verwaltung öffentlicher Schlüssel-Zertifikate, wie sie beispielsweise für einen gesicherten Nachrichtentransport benötigt werden.

Somit wird die Speicherung von Zertifikaten und Widerrufslisten (revocation lists) unterstützt, die von Certification Authorities (CAs) produziert werden können. DirX Directory ist mit Produkten führender CA-Hersteller erfolgreich getestet worden.

Audit Logging

DirX Directory unterstützt die Aufzeichnung von Informationen über die Kommunikation mit seinen Komponenten zur weiteren Auswertung. Die Informationen, die aufgezeichnet werden sollen, sind konfigurierbar. Dazu können u.a. gehören:

- die Identifikationsnummer der Session, um die Verbindung zu identifizieren
- das Protokoll, mit dem der Zugriff

auf den Server stattgefunden hat
- der Name des Zugreifenden, falls bekannt
- die Art der Directory-Operation mit Zeitstempel, Dauer und einer Zusammenfassung seiner Argumente
- das Ergebnis der Operation oder ein Fehlerbericht
- Session Tracking Werte wie Source IP, Source Name

Die Informationen werden in eine Log-Datei geschrieben und können zum Beispiel zur Analyse des Datenverkehrs genutzt werden oder um Abrechnungen zu erstellen.

Audit Logging wird für alle Protokolle sowohl für den DirX Directory DSA als auch für den LDAP-Server unterstützt.

Für die nachfolgende Analyse stehen Kommandos zur Verfügung, die es ermöglichen, die Audit-Daten nach ausgewählten Kriterien zusammenzufassen und zu filtern.

DirX Directory MIBs

DirX Directory unterstützt sowohl MIB Informationen (Management Information Base) basierend auf RFC 2605 und RFC 2788 als auch DBAM-Statistiken.

Diese Informationen, sowohl für den DSA als auch für den LDAP-Server, sind für den Administrator über dirxadm oder DirX Manager abrufbar.

SNMP-Unterstützung

DirX Directory unterstützt das Senden von SNMPv2 Traps an Trap-Empfänger gemäß den RFC 1155 und RFC 1905 Standards.

Das Ein- und Ausschalten sowie die Konfiguration der SNMP Traps erfolgt über eine Konfigurationsdatei.

Die Überwachung des Directory Service mittels SNMP Traps kann das Aufspüren kritischer Situationen unterstützen, bevor ein schwerwiegendes Ereignis eintritt, zum Beispiel der Mangel an Ressourcen.

Nagios-Unterstützung

DirX Directory stellt eine Reihe spezialisierter Nagios-Plugins zur Verfügung, die in einer existierenden Nagios-Umgebung zur Überwachung der Ressourcen der DirX Directory Services und ihrer Operationen sowie zur Sammlung von Statistiken über diese Objekte zur nachfolgenden Analyse genutzt werden können.

Die DirX Directory Nagios Plugins ermöglichen es, wichtige Aspekte des DirX Directory Services zu überwachen. Dazu gehören zum Beispiel:

- Die Ressourcen, die von den DirX Directory Prozessen genutzt werden, wie zum Beispiel Speicherbelegung und File-Deskriptoren
- Die Reaktionsbereitschaft der DirX Directory Prozesse (DSA und LDAP-Server), die entweder alleine oder in Replikationskonfigurationen laufen
- Die Ressourcen und Statistiken, die vom LDAP-Server in seinen MIBs bereitgehalten werden sowie Änderungen dieser Werte im Zeitverlauf
- Ergebnisgrößen von LDAP-Suchoperationen und die Dauer von LDAP-Clientaufrufen
- Die Häufigkeit von DirX Directory Datenbank Backup-Operationen
- Die Kapazität der DBAM Devices, die in einer DirX Directory Installation konfiguriert sind
- Der operative Status der DBAM-Datenbank
- Die Betriebsart des DirX Directory Services

Die DirX Directory Nagios Plugins stellen Eingabeparameter zur Festlegung von Schwellwerten für Warnmeldungen und für Hinweise auf kritische Werte für die überwachten Objekte bereit. Damit wird den Administratoren die Gelegenheit gegeben, auf Probleme, die von den Nagios Plugins über die Nagios-Oberfläche angezeigt werden, zu reagieren, bevor diese kritisch werden und deren Lösung zu überwachen.

Die DirX Directory Nagios Plugins werden als voll funktionsfähige Perl-basierte Module ausgeliefert, die zur Erfüllung spezieller kundenspezifischer Anforderungen zur Überwachung von DirX Directory erweitert werden können.

Hochverfügbarkeits-konfiguration

DirX Directory ist für den Einsatz in Umgebungen vorgesehen, in denen hohe Verfügbarkeit, Skalierbarkeit und Leistung äußerst wichtig sind. Um dazu eine geeignete Plattform zur Verfügung zu stellen, ist entweder eine Software-basierte Lösung oder eine kombinierte und integrierte Hardware- und Software-Lösung nötig.

Als Software-basierte Lösung zur Sicherstellung der Hochverfügbarkeit kann die DirX Directory Shadowing-Funktionalität genutzt werden. Mit DirX Directory kann das sogenannte Floating Master Konzept realisiert werden, wobei ein vollständiger Shadow-Server entweder manuell oder automatisch einfach zu einem Master-Server umgeschaltet werden kann. Damit wird ein durchgängiger Service sowohl für Lese- als auch für Schreib-Operationen zur Verfügung gestellt.

Alternativ bzw. zusätzlich zu einer Software-basierten Strategie zur Sicherstellung der Hochverfügbarkeit kann eine kombinierte und integrierte Hardware- und Software-Lösung realisiert werden. Obwohl es verschiedene Konfigurationsmöglichkeiten für die Lösung gibt, sind drei Komponenten von zentraler Bedeutung:

- ein Cluster-System bestehend aus zwei Knoten
- ein RAID-System, das mit den zwei Knoten verbunden ist
- eine unterbrechungsfreie Stromversorgung (UPS) oder ähnliche Ausrüstung

Cluster-Systeme sind eine Technologie, die eine Reihe von sogenannten Knoten (Server) zu einem einzigen System verbindet, um ein durchgehend verfügbares System bereitzustellen.

Cluster werden ausfallsicher konfiguriert, bestehend aus dem Netzwerk, Cluster Interconnect, Speicher und Software. Anwendungen für Cluster-Systeme wie DirX Directory können als sogenannter Failover Service konfiguriert werden: das Cluster-System ordnet die Anwendung im Fall des Ausfalls eines Knotens automatisch einem anderen Knoten zu. Nicht jeder Fehler muss zu einem Failover zu einem anderen Knoten führen: durch Überwachung der Anwendung mittels Watchdogs und anderer Services kann auch ein Wiederanlauf auf dem gleichen Knoten stattfinden. Der Standby Server kann - sowohl von einer DirX Directory Kopie als auch von einer anderen Anwendung - auch zur Lastverteilung und Verbesserung der Leistung genutzt werden, solange der Primary Server in Betrieb ist.

Die RAID-Technologie (Redundant Arrays of Independent Disks) wird eingesetzt, um die Sicherheit der Daten und die Leistung für die Speicherung großer Datenmengen zu verbessern. Für eine DirX Directory Konfiguration wird das RAID-Level

10 empfohlen. RAID-Level 10 ist eine Kombination von Level 0 (Striping über mehr als zwei Laufwerke, was die Leistung stark verbessert) und Level 1 (Datenspiegelung, bei der die Daten automatisch auf eine zweite Plattenkonfiguration kopiert werden, was die Sicherheit der Daten und deren schnelles Wiederherstellen ermöglicht). Zusätzlich tragen die Spiegelplatten durch die Verdoppelung des Durchsatzes bei Lese-Operationen zur Leistungssteigerung bei.

Supervisor

Das automatische Umschalten in Floating Master Konfigurationen wird durch den Skript-basierten DirX Directory Supervisor unterstützt. Der Supervisor bietet die kontinuierliche und periodische Überwachung der Verbindungen zwischen den in der Konfiguration definierten DirX Directory Master und Shadow Instanzen und der zugrundeliegenden Netzwerkverbindungen. Die Supervisor-Skripte können kundenspezifisch angepasst werden, um die Bedingungen, die zum automatischen Umschalten eines vollständigen Shadow-Servers zu einem Master-Server führen sollen, anzupassen.

Skalierbarkeit

DirX Directory verfügt über eine hochskalierbare Architektur sowohl in Bezug auf die Anzahl der Einträge, die gespeichert werden können, als auch in Bezug auf die Anzahl gleichzeitiger Benutzer und Anfragen, die unterstützt werden.

Skalierbarkeit der Datenbank:

- Ein Server kann mehrere zehn Millionen Einträge speichern und verwalten inklusive aller benötigten Indizes.
- Unter einem Knoten kann eine unbegrenzte Anzahl von Einträgen gespeichert werden.
- Zur optimalen Speicherung großer Attributwerte können Attribute ausgelagert werden.
- Für unbegrenzte Skalierbarkeit können mehrere Server zu einer verteilten Konfiguration zusammengeschaltet werden. Auf den kompletten Datenbestand kann über jeden der Server lesend und schreibend zugegriffen werden.

Skalierbarkeit von Benutzeranfragen und Durchsatz:

- Optimale Indexierung für schnelle und effiziente Suchvorgänge
- Multi-Level Caching, automatisches Vorabladen (Preload) des Cache und entsprechende Konfiguration der Cache-Größen
- Die Multi-Threaded Serverarchitektur erlaubt eine annähernd lineare Skalierbarkeit mit der Anzahl der Prozessoren
- Einsatz von hochperformanten Plattensubsystemen (z.B. RAID 10) bzw. SANs
- Replikation und Verteilung der Daten auf mehrere Server erlauben die Lastverteilung
- Multi-Version DBAM zur Optimierung des Durchsatzes bei Änderungsoperationen ermöglicht eine Änderungsoperation und mehrere Abfrageoperationen parallel
- LDAP- und DSA-Server können auf unterschiedlichen Rechnern eingesetzt werden.
- Zur optimalen Lastverteilung können mehrere LDAP-Server mit demselben DSA verbunden werden oder ein LDAP-Server kann mit mehreren DSAs verbunden werden.

Administration

DirX Directory bietet eine Reihe von Administrationstools:

Die Komponente dirxload ist ein hochleistungsfähiges Tool zum direkten Laden großer Datenmengen in die Datenbank im Offline-Betrieb.

Die Komponente dirxmodify ist ein Tool zum Laden großer Datenmengen über LDAP und zum Überprüfen von Daten.

Die Komponenten dirxadm/dirxcp und die grafische Administrationsoberfläche DirX Manager werden zur Administration von DirX Directory eingesetzt. dirxcp und dirxadm basieren auf der Shell-ähnlichen Kommandosprache Tcl (Tool Command Language). Tcl unterstützt die Benutzung von Variablen, bedingten Anweisungen, Listenverarbeitungsfunktionen, Schleifenbildungen und andere Eigenschaften bekannter Kommandosprachen. Dadurch wird die Realisierung von Shell-Scripts zur Batchverarbeitung und damit ein einfaches Customizing des Systems ermöglicht.

Die Programme dirxcp/dirxadm erweitern diese Funktionen um eine Reihe vordefinierter Kommandos zur Verwaltung von DirX Directory Administrationsobjekten und zur Vereinfachung von Routine-Aufgaben des Administrators.

Es gibt zwei unterschiedliche Modi zur Nutzung von dirxadm/dirxcp:

- Interaktiver Modus, in dem einzelne Kommandos im Dialog eingegeben und deren Ergebnisse angezeigt werden können
- Kommando-Modus, bei dem ganze Kommandofolgen zum Ablauf gebracht werden können.

Das dirxbackup Programm ist ein Tool zum Sichern und Wiederherstellen der DBAM-Datenbank in bzw. aus

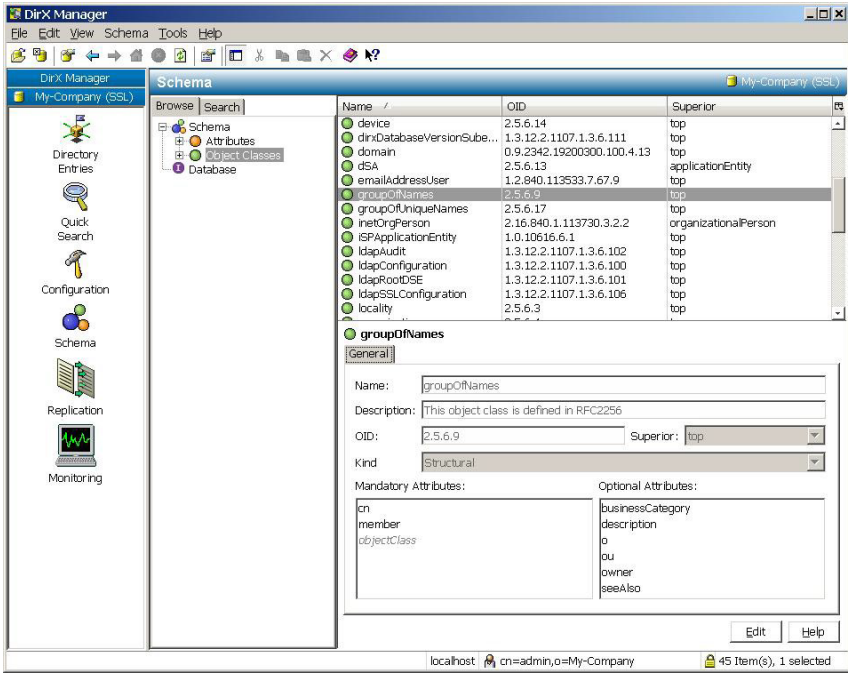

Abbildung 5 - DirX Manager - Schema Management

einem DBAM-Datenbank-Archiv.

Die Komponente dirxload

Die Komponente dirxload dient zum optimierten Laden großer Datenmengen in das Directory im Offline-Betrieb. Beispielsweise kann dirxload für die erstmalige Versorgung des Directory mit bereits vorhandenen Daten genutzt werden oder um nachträglich Daten in das Directory hinzuzufügen. Der Administrator kann eine oder mehrere LDIF Content Files spezifizieren, die direkt in die DBAM Datenbank geladen werden sollen. Wahlweise kann dirxload so konfiguriert werden, dass eine Attributindexierung während des Ladevorgangs durchgeführt wird.

Die Komponente dirxmodify

Das Tool dirxmodify verarbeitet LDIF Content oder Change Files und führt Änderungen im Directory über LDAPv3 aus. Das Tool kann lokal oder von einem entfernten Rechner eingesetzt werden. Das Tool stellt umfangreiche Verarbeitungsoptionen zur Verfügung, die auch im Offline-Betrieb eingesetzt werden können, um LDIF Files zu überprüfen oder um Statistiken zu erstellen. Im Einzelnen gehören dazu:

- Unterstützung von anonymen und simple authenticated Bind zum LDAP-Server
- Konvertierung von ISO-8859-1 Zeichen in UTF-8 Zeichen
- Überprüfung von LDIF Files auf syntaktische Korrektheit und Anzeige von Statistiken über Attribute, Einträge und Knoten in den Dateien im Offline-Betrieb
- Ausführen einfacher Anfragen direkt auf der LDIF-Datei

Ersetzen von Attribut-Werten und –Typen beim Übertragen von der Datei in das Directory

Weglassen ausgewählter Attribute beim Laden

Die Komponente dirxcp

Das Tool dirxcp ist ein Kommando-basierter Directory Client, den Administratoren oder Anwender benutzen können, um mit einem LDAP-Server über LDAP oder mit einem DSA über DAP zu kommunizieren. Es wird eingesetzt zum:

- Senden von Anforderungen an DSAs, um Operationen wie Erzeugen neuer Objekte, Ändern, Löschen und Suchen nach Objekten/Einträgen im Directory Information Tree (DIT) auszuführen
- Ausführen von Abfragen zu Objekten im DIT
- Ändern von Parametern, um das Verhalten der Operationen zu ändern
- Anzeigen der Abkürzungen, die für die Attribute und Object Identifier benutzt werden.

Die Komponente dirxadm

Das Tool dirxadm ist ein Satz von Kommandos, mit denen der Systemadministrator die LDAP-Server und DSAs verwalten kann, zum Beispiel DSA-spezifische Einträge (DSEs) und operationale Attribute. Die Kommandos bieten folgende Funktionen:

- Administration der lokalen DSE und DSA Policies.
- Administration der Verbindungen zwischen zwei DSAs (Operational Bindings für Replikations-Events und die Verteilung von Directory-Daten zwischen zwei DSAs).
- Konfiguration der Datenbasis, die vom DSA benutzt wird
- Anzeigen von Monitoring-Informationen, die in der Management Information Base des DSA abgelegt sind
- Durchführung von Administrationsaufgaben, wie
- Starten und Beenden der Server und
- Ein-/Ausschalten des Logging

Die Komponente dirxbackup

DirX Directory stellt Funktionen zur vollständigen Sicherung oder zur Differenz-Sicherung zur Verfügung, ohne dass der Service unterbrochen wird. Sowohl Such- als auch Änderungsoperationen sind während der Sicherung erlaubt.

Das Tool dirxbackup dient zum Sichern, Wiederherstellen und Verifizieren einer DBAM Datenbank. Es kann in Verbindung mit einem Daten-Komprimierungs-/Dekomprimierungs-Tool wie beispielsweise gzip genutzt werden.

Folgende Funktionen stehen zur Verfügung:

- Sichern einer DBAM-Datenbank in einem Datenbankarchiv
- Wiederherstellen einer DBAM-Datenbank aus einem Datenbankarchiv
- Verifizieren eines Datenbankarchivs auf Konsistenz

DirX Manager

Mit dem Java-basierten LDAP Management Client DirX Manager wird eine konfigurierbare, Plattform-unabhängige grafische Administrationsoberfläche zur Verwaltung lokaler und entfernter DirX Directory Server zur Verfügung gestellt.

Die wesentlichen Funktionen von DirX Manager sind:

- Verwaltung von Directory-Einträgen (hinzufügen, löschen, ändern)
- Browsen und Suchen im Directory
- Schema-Management über LDAP
- Replikationsmanagement über RPC
- Anzeige von Indizes
- Verwaltung und Anzeige der Subentry Informationen
- Verwaltung der Passwort-Policies
- Verwaltung der Proxied Authorization Controls
- Directory Monitoring View für den LDAP-Server and den DSA über erweiterte LDAP-Operation
- Verwaltung mehrerer Server
- Import von LDIF Content und Change Files und von DSMLv1 und DSMLv2 Files in das Directory
- Export von ausgewählten Directory-Inhalten in DSMLv1, DSMLv2 Files oder LDIF Content Files
- SSL Server Authentisierung
- Kundenspezifisch anpassbare logische Sichten
- Erstellung von Scripts und Ausführung von dirxcp und dirxadm uas der grafischen Oberfläche
- Unterstützung von Simple Paging

Logging von System-Events

In DirX Directory werden zwei Ebenen der Programmüberwachung angeboten:

- Fehler- und Statusreports des Systems
- Kontrolle des Programmablaufs

Der Administrator kann konfigurieren, welche Meldungen protokolliert werden und in welcher Form und wo sie gespeichert werden. Auf UNIX-Systemen können Fehler- und Statusmeldungen an den Unix syslog Daemon weitergeleitet werden.

RESTful API

DirX Directory verfügt über einen http-Server namens dirxhttp als Teil des Dienstes. Er ermöglicht den Zugriff auf den DIT (Directory Information Tree) über das HTTP-Protokoll. REST-Aufrufe (Representational State Transfer) an den dirxhttp-Server verwenden ein benutzerdefiniertes JSON-Schema (JavaScript Object

Notation) für den Datenaustausch, das die Kommunikation sichtbar macht.

Die Dokumentation wird in der OpenAPI v3.0-Notation bereitgestellt und ermöglicht auch die interaktive Nutzung der RESTful API, z.B. zu Testzwecken.

Corporate Directory App

Um die Funktionen der RESTful API zu darzustellen, verfügt DirX Directory über eine benutzerzentrierte Webanwendung mit responsivem Design auf Basis von Angular.

Diese bietet Unternehmensverzeichnisfunktionen wie das Durchsuchen und Suche nach Benutzerdaten, außerdem erlaubt es Anwendern, bestimmte Bereiche ihrer Daten zu verwalten.

Integration auf Windows Plattformen

Auf Windows Plattformen ist die Administration von DirX Directory an die spezielle Systemumgebung angepasst integriert:

- Anzeige der Logging-Informationen mit dem Event-Viewer
- DirX Directory läuft als Windows Service und kann über die Windows Service-Administration verwaltet werden

Unterstützung von 64-Bit-Architekturen

DirX Directory läuft als 64-Bit-Anwendung auf Red Hat Enterprise Linux, SUSE Linux Enterprise Server, sowie unter Microsoft Windows Server auf x86-64 Architekturen (Intel).

Containerisierte Bereitstellung

DirX Directory kann in einer Containerumgebung ausgeführt werden, die auf einer Kubernetes-Distribution basiert.

Es bietet außerdem ein Beispiel-Container-Image, das in einer Docker-Container-Laufzeitumgebung ausgeführt werden kann.

Konformität zu Standards und Interoperabilität

DirX Directory ist konform zu den Internet LDAP Standards: RFCs 1155, 1274, 1277, 1905, 2222, 2247, 2279, 2377, 2559, 2587, 2596, 2696, 2798, 2849, 2891, 3045, 3673, 4370, 4510, 4511, 4512, 45131, 4514, 4515, 4516, 4517, 45182, 4519, 4529, 6171

MIB-Informationen basierend auf RFC 26053 und 27883

DirX Directory ist konform zu den folgenden ITU-T und ISO/IEC Standards:

ITU-T X.500, X.501, X.511, X.518, X.519, X.520, X.521, X.509, X.525

ISO/IEC 9594-1, 9594-2, 9594-3, 9594-4, 9594-5, 9594-6, 9594-7, 9594-8, 9594-9

1993er Profile:

ADY11, ADY12, ADY21, ADY22, ADY41, ADY42, ADY43, ADY44, ADY45, ADY51, ADY53,

FDY11, FDY12

Zusätzlich zum IPv4-Protokoll unterstützt DirX Directory IPv6 für die folgenden Protokolle

- LDAP
- X.500 DAP/DSP/DISP (IDM-basiert)

Über die Konfigurationsschnittstelle kann der Administrator die IP-Version für den eingehenden und den ausgehenden Verkehr festlegen.

Der dirxhttp Server verwendet die Standards: http, REST, JSON, OpenAPI v3.0

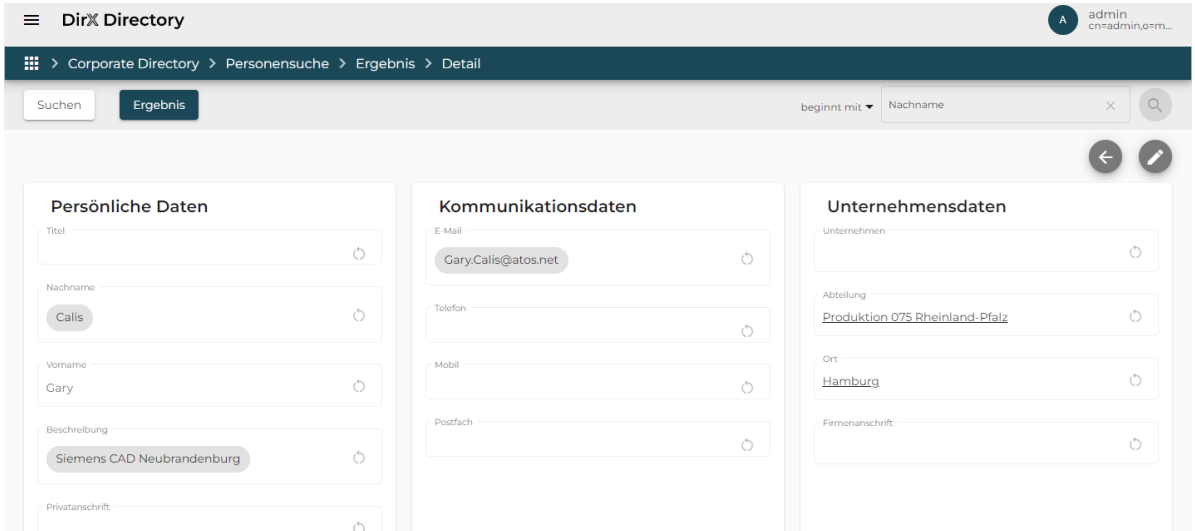

Abbildung 6 - DirX Corporate Directory Applikation

Technische Voraussetzungen

Hardware

- Intel server platform für Microsoft Windows Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server

Speicherbedarf:

Hauptspeicher: mindestens 8 GB

Plattenspeicher: mindestens 4 GB plus Speicher für Daten

Software

- Microsoft Windows Server 2019 und Windows Server 2022
- Red Hat Enterprise Linux Server 8 und 9 (x86-64)
- SUSE Linux Enterprise Server 12 und 15 (x86-64)
- Microsoft Windows 10 und Windows 11 (x86-64, DirX Manager only)

jeweils mit den aktuellen Patches/ Service Packs für die gewählte Plattform

Unterstützung von Cluster-Konfigurationen sind auf Anfrage verfügbar.

Unterstützung virtueller Maschinen:

- VMWare ESXi in Kombination mit den obengenannten Gast-Betriebssystemen, die für VMWare ESXi freigegeben sind

Für DirX Manager

- Java SE Runtime Environment 11 (Abhängigkeiten zur gewählten Betriebssystemplattform sind zu beachten)
- Für die Smartcard-Unterstützung: Atos CardOS API V5.3/V5.4 in Kombination mit Smartcards, die von Atos CardOS API V5.3/V5.4 unterstützt werden

Für DirX Corporate Directory

- Mozilla Firefox 115.3.1esr or newer
- Google Chrome 117.0 or newer
- Microsoft Edge 117.0 or newer

Für Supervisor

- Perl und perl-ldap Distribution aktuelles Release
- Für Windows: Perl 5.16.3 oder neuer
- Für Linux: Perl 5.8 oder neuer

Für Nagios Integration

- Nagios Core Version 3.4.4
- Perl und perl-ldap Distribution aktuelles Release
- Für Windows: Perl 5.16.3 oder neuer
- Für Linux: Perl 5.8 oder neuer

Benutzeroberfläche

- Englisch

Dokumentation

Manuale werden in Englisch bereitgestellt.

Manuale

Folgende DirX Directory Dokumente sind elektronisch angeboten als PDF:

- Introduction Guide
- Administration Guide
- Administration Reference
- Disc Dimensioning Guide
- External Authentication
- LDAP Proxy
- LDAP Extended Operations
- Manager Guide
- Plugins for Nagios
- Supervisor
- Syntaxes and Attributes
- Guide for CSP Administrators
- Best Practices for Database Error Recovery
- Containerization

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