okta

VERZEICHNISINTEGRATION MIT OKTA

Überblick über die Architektur

Okta Deutschland
Oskar-von-Miller-Ring 20
80333 München

info_germany@okta.com
+49 (89) 26203329

Benutzerverzeichnisse und die Cloud: Ein Überblick

Directory Access Protocol) wie SunOne oder Oracle Internet Directory die zentrale Rolle bei der Koordination von Richtlinien für das Identitäts- und Zugriffsmanagement. AD/LDAP dient typischerweise als verlässliche Informationsquelle („Source of Truth“) für Benutzeridentitäten und sorgt für die Kontrolle des Zugriffs auf lokale Ressourcen wie Netzwerke, Dateiserver und Webanwendungen (siehe Abbildung 1). Wenn lokale Anwendungen in Active Directory oder LDAP integriert werden, profitieren Benutzer von bestmöglichem Bedienkomfort: Sie melden sich einmalig an ihrer Domäne an und erhalten Zugriff auf die entsprechenden Ressourcen. Auch die Administratoren profitieren: Sie behalten die klare Kontrolle darüber, wer Zugriff worauf hat. Dieses Modell ist allgegenwärtig, da es gut mit LAN-Architekturen harmoniert (wo Anwendungen auf Hardware innerhalb der Firewall gehostet werden). Aber wie wir zeigen werden, stößt dieser Ansatz an Grenzen, wenn Unternehmen auf Cloud-Anwendungen umsteigen und eine neue Lösung benötigt wird.

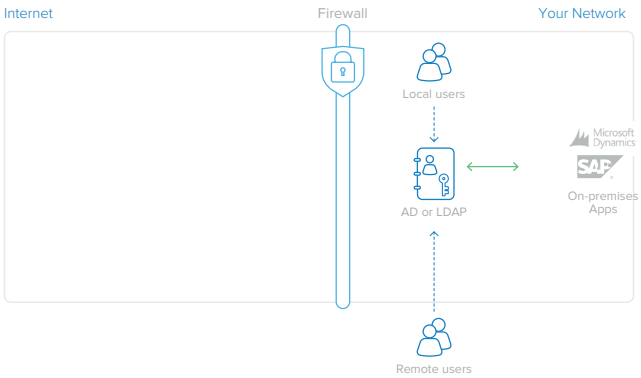

Abbildung 1: AD oder LDAP für lokale Benutzeridentitäten von Anwendungen vor Ort

Ein Nebenprodukt der Umstellung auf Cloud-Anwendungen ist die starke Zunahme separater Benutzerspeicher. Jede Cloud-Anwendung wird typischerweise unabhängig bereitgestellt und verfügt daher über eine eigene zentrale Datenbank mit Benutzer-Anmeldedaten (siehe Abbildung 2). Bei einer oder zwei Anwendungen ist dieser Mehraufwand vernachlässigbar, aber da Unternehmen immer mehr Cloud-Anwendungen einsetzen, sind Administratoren mit einer schwer beherrschbaren Anzahl von verschiedenen Benutzerverzeichnissen konfrontiert. Und dieses Problem wird immer gravierender: Der Wildwuchs der Passwörter nimmt mit jeder neuen Anwendung zu und Administratoren verlieren schnell die Kontrolle darüber, wer Zugriff worauf hat. Schlimmer noch: Wenn ein Mitarbeiter ausscheidet, können die meisten Unternehmen weder einfach und genau feststellen, welche Konten deaktiviert werden müssen, noch verfügen sie über Auditfunktionen, mit denen sie einen rechtzeitigen Entzug von Berechtigungen gewährleisten können.

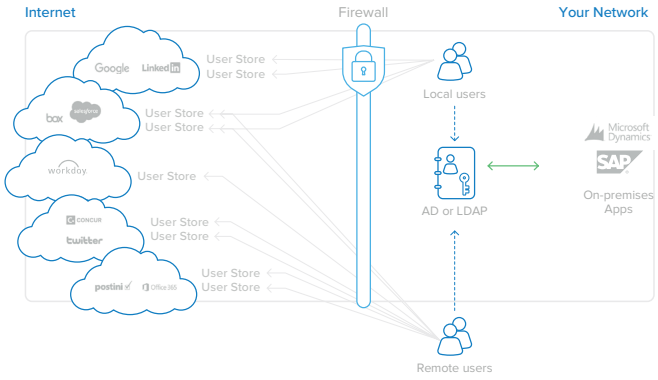

Abbildung 2: Die Übernahme von Cloud-Anwendungen führt zu einer starken Zunahme von Benutzerspeichern

Eine Lösung für das Problem der starken Zunahme unabhängiger Benutzerspeicher ist die Zusammenführung aller Cloud-Anwendungen in einem zentralen Identitätsspeicher (siehe Abbildung 3). AD- oder LDAP-Benutzerspeicher sind hierfür mit Abstand die bequemsten Optionen, da sie das Identitätsmanagement für lokale und für Cloud-Anwendungen gleichermaßen übernehmen können. Einige Anbieter von Cloud-Anwendungen stellen APIs oder Toolkits zur

Verfügung, mit denen Unternehmen versuchen können, die eigenständigen Identitätsspeicher der Anwendung mit AD oder LDAP zu verbinden. Die Integration über APIs erfordert jedoch eine kundenspezifische Entwicklung. Jeder der Toolkits ist indessen unterschiedlich und kann oft erhebliche Investitionen für Einrichtung, Ausrüstung (Hardware zum Ausführen der Konnektorsoftware) und Pflege erfordern, da sich die Anwendungen im Laufe der Zeit ändern. Mit zunehmender Anzahl von Cloud-Anwendungen wird dieses Modell der AD- oder LDAP-Integration pro Anwendung unrentabel: Es gibt immer eine nächste neue Anwendung, die das Unternehmen benötigt.

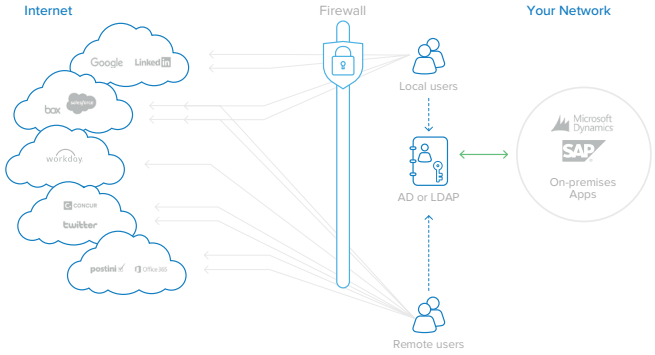

Abbildung 3: Die Anbindung von mehreren Cloud-Anwendungen ist kostspielig und wartungsaufwendig

Oktas Cloud-Identitäts- und Zugriffsmanagementdienst löst diese Probleme durch einen zentralen Integrationspunkt, der eine hochverfügbare Lösung für alle AD- und LDAP-Anbindungen von Cloud- und Web-Anwendungen bietet. Okta beseitigt die Fallstricke, die mit der Eigenentwicklung und Verwaltung von mehreren lokalen Verzeichnisintegrationen verbunden sind:

Fallstricke bei AD/LDAP-Integrationen in Eigenentwicklung	Ansatz von Okta
Haben Sie Mitarbeiter mit den nötigen Fähigkeiten, um Integrationen zu entwickeln?	Mit Okta erfordern Integrationen keine Programmier- oder Entwicklungserfahrung und können über unsere benutzerfreundliche Oberfläche in wenigen Minuten durchgeführt werden.
Wie gewährleisten Sie Upgrades und die Pflege von Integrationen?	Okta arbeitet mit Softwareherstellern zusammen und überwacht Änderungen und Upgrades an bestehenden APIs, um die Vorteile der neuesten Funktionen zu nutzen. Wir veröffentlichen wöchentlich Updates, um Änderungen zu berücksichtigen.
Wie überwachen Sie die Betriebsbereitschaft der Integration?	Okta überwacht und testet kontinuierlich bestehende Integrationen, damit die Integration nach Upgrades und Releases wie erwartet funktioniert.
Welches Protokoll verwenden Sie für die Verbindung zu der jeweiligen Cloud-Anwendung?	Mit Okta sind keine Expertenkenntnisse von SAML, OAuth, SCIM und diversen anderen Integrationsprotokollen erforderlich, da Okta diese Integrationen für Sie verwaltet.
Was passiert, wenn der Server ausfällt, auf dem die selbst entwickelte, auf einem Toolkit aufbauende Integration läuft?	Okta sorgt für eine automatische Ausfallsicherung mit einer redundanten Agentenarchitektur.
Wie binden Sie Ihre Cloud-App an eine AD- oder LDAP-Konfiguration mit mehreren Domänen an?	Okta bietet eine integrierte Unterstützung für mehrere AD- und/oder LDAP-Domänenumgebungen.
Welche Änderungen an der Firewall sind für jede Anbindung von Cloud-Anwendungen an AD/LDAP erforderlich?	Mit Okta sind keine Änderungen an der Firewall erforderlich, um AD- oder LDAP-Anbindungen zu unterstützen.

Gleich nach der Einrichtung bietet Okta eine Infrastruktur, mit der Unternehmen neue Cloud-Anwendungen nach Belieben einführen können, während sie weiterhin interne Verzeichnisse für die Benutzeridentitäten ihrer Mitarbeiter nutzen. Auf diese Weise können Benutzer mit ihren vorhandenen AD- oder LDAP-Anmeldedaten auf sämtliche Cloud-Anwendungen zugreifen. IT-Administratoren können den Zugriff auf diese Anwendungen über eine zentrale Bedienoberfläche steuern. Dabei werden AD- oder LDAP-Sicherheitsgruppen mit individuellen Benutzerzuordnungen kombiniert.

Okta-Verzeichnisintegration für alle Cloud-Anwendungen

Okta bietet eine komplette und einfach zu bedienende Verzeichnisintegrationslösung für Cloud- und lokale Webanwendungen. Der On-Demand-Identitäts- und Zugriffsverwaltungsdienst von Okta bietet Benutzerauthentifizierung, Erteilung und Entzug von Benutzerrechten sowie detaillierte Analysen und Berichte über die Anwendungsnutzung sowohl für Cloud-Anwendungen als auch für lokale Webanwendungen. Eine Schlüsselkomponente dieses Dienstes ist die Verzeichnisintegration von Okta, die sehr einfach einzurichten und auf Hochverfügbarkeit ausgelegt ist. Darüber hinaus verwaltet Okta die verschiedenen Integrationen für Sie, wobei Tausende von Anwendungen im Application Network (OAN) von Okta unterstützt werden.

Für die AD-Integration stellt Okta drei sichere Komponenten mit geringem Ressourcenbedarf für die Installation vor Ort zur Verfügung:

- **Okta Active Directory Agent:** Ein Agent mit geringem Ressourcenbedarf, der auf jedem Windows Server installiert werden kann und zur Verbindung mit dem lokalen Active Directory für die Erteilung und den Entzug von Berechtigungen sowie für Authentifizierungsanfragen verwendet wird.
- **Okta Webanwendung Integrated Windows** Authentication (IWA): Eine Webanwendung mit geringem Ressourcenbedarf, die auf einem IIS-Server (Internet Information Services) installiert ist und zur Authentifizierung von Domänenbenutzern über die integrierte Windows-Authentifizierung verwendet wird.
- **Okta Active Directory Password Sync Agent:** Ein Agent mit geringem Ressourcenbedarf, der auf den Domänencontrollern installiert wird und automatisch AD-Passwortänderungen synchronisiert, an Okta sendet und die AD-Passwörter der Benutzer mit den von ihnen verwendeten Anwendungen synchronisiert.

Für die LDAP-Integration stellt Okta eine sichere Komponente mit geringem Ressourcenbedarf für die Installation vor Ort zur Verfügung:

- **Okta LDAP-Agent:** Ein Agent mit geringem Ressourcenbedarf, der auf jedem Windows Server installiert werden kann und zur Verbindung mit lokalen LDAP-Benutzerspeichern für die Erteilung und den Entzug von Benutzerberechtigungen sowie für Authentifizierungsanfragen verwendet wird.

Die AD/LDAP-Agenten, die IWA-Webanwendung und der AD Password Sync Agent von Okta bilden zusammen mit dem Cloud-Dienst von Okta eine hochverfügbare, einfach einzurichtende und zu wartende Architektur, die mehrere Anwendungsfälle abdeckt. Das vorliegende Whitepaper enthält zusätzliche Details zu dieser flexiblen Architektur.

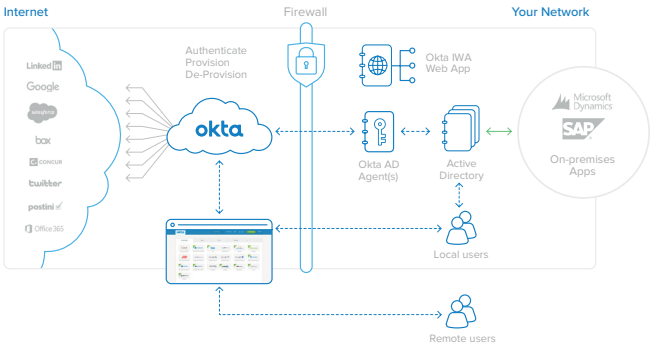

Abbildung 4: Architektur von Okta für Active Directory: Eine Integration für alle Webanwendungen

Die Okta-Verzeichnisintegration bietet folgende Vorteile:

- **Einfache und sichere Einrichtung und Konfiguration**
- **Echtzeit-Bereitstellung**
- **Intelligente Benutzersynchronisierung**
- **Just-in-Time-Erteilung von Benutzerberechtigungen**
- **Zuverlässige delegierte Authentifizierung**
- **Integriertes Single-Sign-On (SSO) für den Desktop (nur AD)**
- **Unterstützung für Self-Service-Passwortrücksetzung (nur AD)**
- **Erteilung von Berechtigungen auf Basis von Sicherheits-Gruppen**
- **Automatisierter One-Klick Entzug von Berechtigungen**
- **Single Sign-On für per Verzeichnis authentifizierte Anwendungen**

Einfache und sichere Einrichtung und Konfiguration

Mit Okta ist die Aktivierung der Verzeichnisintegration ein einfacher, von einem Assistenten unterstützter Prozess. Mit einem Klick von der Okta-Administrationskonsole aus können Sie den AD- oder LDAP-Agenten von Okta herunterladen und auf einem Windows-Server installieren, der Zugriff auf den Domänencontroller hat. Die Okta-Agenten werden auf einem von dem Domänencontroller getrennten Server ausgeführt.

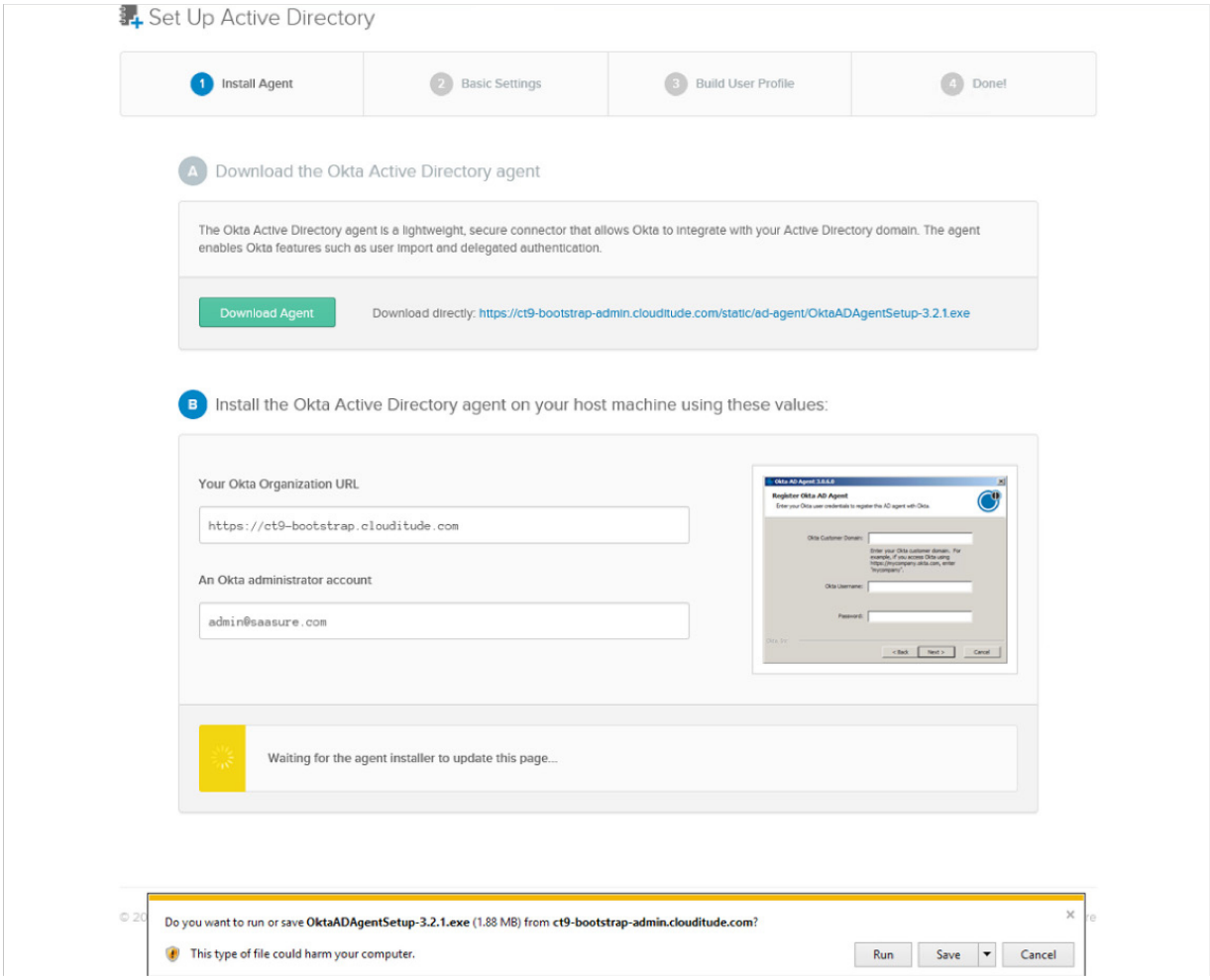

Abbildung 5: Der Active-Directory-Installationsprozessy

Während der Installation geben Sie einfach Ihre Okta-URL und die Anmeldedaten des AD-Administrators ein. Der AD-Agent von Okta erstellt ein schreibgeschütztes Integrationskonto mit niedriger Berechtigung und stellt dann eine sichere Verbindung zu Ihrer Okta-Instanz her. Eine Netzwerk- oder Firewall-Konfiguration ist nicht erforderlich.

Der AD-Agent von Okta verbindet sich mit dem Cloud-Dienst von Okta über eine ausgehende SSL-Verbindung zu Port 443. Diese Verbindung wird alle 30 Sekunden unterbrochen, um die Kompatibilität mit bestehenden Firewalls oder anderen Sicherheitsvorrichtungen sicherzustellen. Als Faustregel gilt: Wenn sich ein Benutzer mit AD-Anmeldedaten am Host anmelden und über einen Browser auf das Internet zugreifen kann, wird auch der AD-Agent funktionsfähig sein und keine Änderungen an der Firewall erfordern.

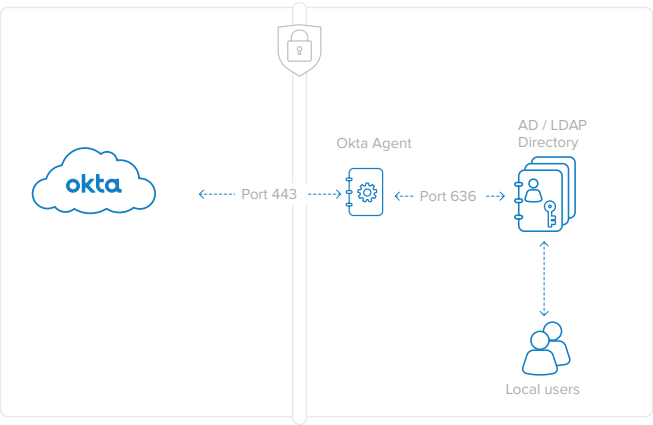

Abbildung 6: Die Verbindungen des Okta-Agenten erfolgen über Port 443 für AD (mit SSL verschlüsselt) und über Port 636 für LDAP. Es sind keine Änderungen an der Firewall erforderlich – weder für den AD- noch für den LDAP-Agenten.

Die Kommunikation mit den AD/LDAP-Agenten von Okta ist durch SSL und gegenseitiger Authentifizierung abgesichert:

- **AD/LDAP-Agenten an Okta-Dienst:** Der Agent authentifiziert den Dienst, indem er das Okta-Server-SSL-Zertifikat für mein_unternehmen.okta.com validiert. Der Dienst authentifiziert den Agenten mithilfe eines Sicherheitstokens, das dem Agenten bei der Registrierung zur Verfügung gestellt wird. Der Registrierungsprozess erfordert die Anmeldedaten des Okta-Administrators, um das Sicherheitstoken zu generieren. Das Sicherheitstoken gilt jeweils für einen einzigen Agenten und kann jederzeit widerrufen werden.
- **Okta-Agent zum Domänencontroller oder LDAP-Server:** Der Agent authentifiziert sich am Domänencontroller mit dem schreibgeschützten Integrationskonto mit niedriger Berechtigung, das während des Installationsprozesses des Agenten erstellt wurde.

Echtzeit-Synchronisierung

Abweichungen der Profildaten zwischen dem Benutzerspeicher und Okta, wie sie beim Import von Profildaten nach Zeitplan auftreten können, sind kein Thema: Dank Echtzeitsynchronisierung aktualisiert Okta die Profile bei jeder Anmeldung nahtlos. Ob einzelne Profildaten oder die Daten größerer Gruppen geändert wurden, ist dabei unerheblich. Die Benutzerdaten werden von Okta rund um die Uhr laufend aktualisiert.

Die Echtzeitsynchronisierung wird folgendermaßen aktiviert:

1. **Laden Sie den entsprechenden Agenten herunter und installieren Sie ihn.**
2. **Importieren sie OUs und Gruppen (ohne die Mitgliederattribute).**
3. **Konfigurieren Sie die OU-Auswahl und die Einstellung für den Benutzernamen. Hinweis: Im Pulldown-Menü für den Import nach Zeitplan wird „Nie“ eingestellt.**
4. **Delegierte Authentifizierung und Just-in-Time-Erteilung (JIT) von Benutzerberechtigungen sind standardmäßig aktiviert.**
5. **Benutzer können ohne vorherigen Import sofort JIT nutzen und Okta-Benutzer werden.**
6. **Bei jeder delegierten Authentifizierung und JIT-Anfrage werden zusätzlich zum vollständigen Benutzerprofil auch Gruppenmitgliedschaften importiert.**

7. **Die Benutzer werden bei jeder Anmeldung vollständig und asynchron aktualisiert.**

Administratoren können OUs, Benutzerprofile und Gruppeninformationen in Active Directory ändern, und die Benutzer werden vollständig aktualisiert.

Just-in-Time-Erteilung von Benutzerberechtigungen

Die Erteilung von Benutzerberechtigungen ist mit Oktas Just-in-Time-Funktion sehr einfach und schnell. Mit der Just-in-Time-Erteilung von Benutzerberechtigungen können IT-Administratoren die automatische Erstellung neuer Benutzerkonten in Okta ermöglichen, sofern diese bereits im Active Directory oder in einem LDAP-Benutzerspeicher vorhanden sind.

IT-Administratoren brauchen vor der Aktivierung von Benutzerkonten keinen Erstimport durchzuführen, das spart Zeit bei der Konfiguration. Benutzer können sich sofort bei Okta anmelden, indem sie ihre Anmeldeseite aufrufen und sich mit ihren Verzeichnis-Anmeldedaten (AD oder LDAP) anmelden. Administratoren können das vollständige Benutzerprofil, die Gruppen und die Gruppenmitgliedschaften auf der Registerkarte „People“ (Personen) einsehen.

Die Just-in-Time-Bereitstellung erfolgt folgendermaßen:

1. **Ein Benutzer, der bisher nicht vom Okta-Dienst bereitgestellt wurde, versucht, sich bei mein_unternehmen.okta.com anzumelden.**
2. **Okta und der Okta-Agent überprüfen die Benutzerdaten anhand von Active Directory oder LDAP.**
3. **Wenn der Benutzer in AD/LDAP aktiv ist, wird automatisch ein neues Benutzerkonto in Okta erstellt. Das neue Benutzerkonto nutzt die vorhandenen AD-Anmeldedaten.**
4. **Abhängig von den Attributen der Verzeichnissicherheitsgruppe wird das Benutzerkonto über den Okta-Dienst automatisch für nachgelagerte Cloud- und Webanwendungen bereitgestellt.**

Die Just-in-Time-Bereitstellung ermöglicht es IT-Administratoren, die Benutzerakzeptanz sowohl des Okta-Dienstes als auch aller zugeordneten Cloud-Anwendungen zu erhöhen und gleichzeitig die AD- bzw. LDAP-Anmeldedaten bereits vorhandener Benutzer zu nutzen.

Bedienerfreundliche delegierte Authentifizierung

Mit der Verzeichnisintegration von Okta haben Sie auch die Möglichkeit, die Authentifizierung von Benutzern in Okta an eine lokale AD- oder LDAP-Domäne zu delegieren. Das heißt, jede versuchte Benutzeranmeldung bei mein_unternehmen.okta.com wird zur Authentifizierung über Active Directory oder LDAP geprüft. Benutzer können sich dann ganz einfach mit ihrem Okta-Benutzernamen und ihrem Verzeichnispasswort bei Okta anmelden.

Der Vorgang läuft wie folgt ab:

1. **Der Benutzer gibt seinen Benutzernamen und sein Passwort auf der Benutzer-Startseite von Okta ein. Diese Anmeldeseite ist mit SSL und einem Sicherheitsbild vor Phishing geschützt. Eine Multi-Faktor-Authentifizierung (zusätzliche Sicherheitsfrage oder Soft-Token per Smartphone) kann ebenfalls aktiviert werden.**
2. **Der Benutzername und das Passwort werden an einen Okta Directory Agent übermittelt, der hinter der Firewall über die SSL-Verbindung läuft, die zuvor bei der Einrichtung erstellt wurde.**
3. **Der Okta Directory Agent übergibt diese Anmeldedaten zur Authentifizierung an den AD- oder LDAP-Domänencontroller.**

4. **Der Domänencontroller antwortet mit einer Ja/Nein-Antwort und überprüft den Benutzernamen und das Passwort.**
5. **Die Ja/Nein-Antwort wird vom Okta Directory Agent an den Okta-Dienst zurückgesendet. Wenn ja, wird der Benutzer authentifiziert und auf seine persönliche Okta-Startseite („Meine Anwendungen“) weitergeleitet.**

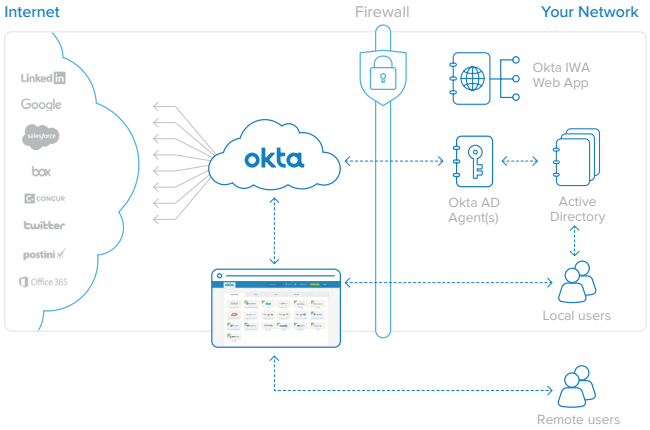

Figure 7 : Délégation de l’authentification à Active Directory

Für Benutzer gestaltet sich die an AD/LDAP delegierte Authentifizierung ganz einfach:

1. **Die Benutzer melden sich auf der Okta-Startseite an und starten die Anwendung.**
2. **Okta greift auf ein Verzeichnis zu, um die Benutzer zu authentifizieren.**
3. **Bei gültiger Authentifizierung werden Okta SSOs in Cloud-Anwendungen eingebunden.**

Da diese Funktion den Benutzerzugriff auf Okta regelt, unterstützt die Architektur mehrere Okta-AD- und/oder LDAP-Agenten, die in Ihrer Umgebung laufen, um Redundanz zu gewährleisten. Wenn einer der AD- oder LDAP-Agenten ausfällt oder die Netzwerkverbindung unterbrochen wird, werden die Authentifizierungsanfragen automatisch an die anderen AD- oder LDAP-Agenten weitergeleitet.

Bei diesem Authentifizierungsmechanismus wird das Passwort des Benutzers niemals im Okta-Dienst gespeichert und Ihr Verzeichnis wird als unmittelbare und verbindliche Datenquelle für die Überprüfung von Anmeldedaten verwendet. Da bei der Benutzerauthentifizierung immer auf AD oder LDAP zurückgegriffen wird, werden Statusänderungen des Benutzers (z. B. Passwortänderungen oder Deaktivierungen) sofort im Okta-Dienst berücksichtigt.

Single Sign-On für den Desktop

Okta unterstützt Single Sign-On für den Desktop und erweitert die Verfahren für die Anmeldung an der Windows-Domäne, um lokalen Benutzern den Zugriff auf Okta und Cloud-Anwendungen zu ermöglichen. Die AD-Integration von Okta verwendet die integrierte Windows-Authentifizierung von Microsoft, um Benutzer, die bereits über ihre Anmeldung an der Windows-Domäne authentifiziert sind, nahtlos bei Okta zu authentifizieren: Sie laden einfach die IWA-Webanwendung von Okta herunter und installieren sie, konfigurieren die relevanten IP-Bereiche und schon ist die Einrichtung abgeschlossen.

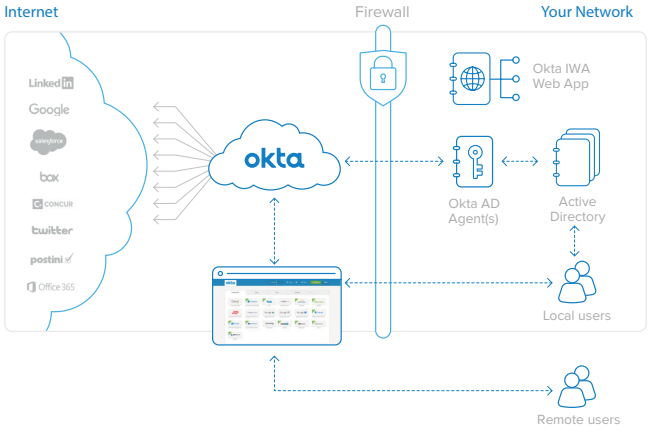

Abbildung 8: Desktop-SSO mit der IWA-Webanwendung von Okta

Die technischen Schritte, die eine nahtlose Anmeldung am Okta-Dienst über Single Sign-On für den Desktop (dargestellt in Abbildung 9) ermöglichen, sind folgende:

1. **Der Benutzer navigiert zu https://mein_unternehmen.okta.com.**
2. **Der Benutzer wird auf die lokal installierte IWA-Webanwendung umgeleitet.**
3. **Die IWA-Webanwendung authentifiziert den Benutzer transparent über die integrierte Windows-Authentifizierung (Kerberos).**

4. **Der Benutzer wird mit kryptographisch signierten Assertionen, die seine AD-Benutzeridentität enthalten, zurück zur Okta-Login-Seite geleitet.**
5. **Der Okta-Dienst validiert die signierten Assertionen und leitet den Benutzer direkt auf seine Okta-Startseite weiter.**

Beachten Sie, dass alle oben genannten Schritte für den Benutzer transparent sind. Die Benutzerfreundlichkeit ist hoch: Der Benutzer navigiert zu https://mein_unternehmen.okta.com und landet sofort auf der seiner Startseite mit Links zu allen ihm zugewiesenen Anwendungen. Alternativ kann ein Benutzer einfach auf einen Link klicken, der einer bestimmten Anwendung entspricht, und sich dann automatisch bei dieser Anwendung anmelden. Die Authentifizierung gegenüber AD hinter den Kulissen ist für den Benutzer transparent.

Schließlich finden Remote-Benutzer oder im Außendienst tätige Benutzer weiterhin SSO in allen Cloud-Anwendungen, indem sie einfach die Benutzer-Startseite von Okta besuchen.

Unterstützung für Self-Service-Passwortrücksetzung

Benutzer können ihr Active-Directory-Passwort auch über Okta ändern. Wenn das AD-Passwort eines Benutzers abläuft oder zurückgesetzt wird, erhält er automatisch eine Aufforderung, es bei der nächsten Anmeldung bei Okta zu ändern. Benutzer können ihr AD-Passwort auch proaktiv direkt auf der Registerkarte „Account“ auf ihrer Okta-Startseite ändern. Okta synchronisiert alle Anmeldedaten mit AD.

Sicherheitsgruppenabhängige Bereitstellung

Der Dienst von Okta verfügt über eine Gruppenfunktion, die zur Steuerung der Massenbereitstellung von Anwendungen und zur Zuweisung an Okta-Benutzer nach Gruppenzugehörigkeit verwendet werden kann. Mit Okta können Sie Active Directory oder die Sicherheitsgruppen von LDAP den nativen Okta-Gruppen zuordnen und somit Benutzern automatisch Anwendungen basierend auf ihrer Mitgliedschaft in AD- oder LDAP-Sicherheitsgruppen bereitstellen.

Wenn Sie einen Benutzer zum Verzeichnis hinzufügen, können Sie ihn einer Sicherheitsgruppe zuweisen. Bei der automatischen Synchronisierung mit Okta wird dieser Benutzer dann hinzugefügt, wobei Konten in den Anwendungen, die dieser Sicherheitsgruppe zugeordnet sind, automatisch bereitgestellt werden. Anwendungsspezifische Parameter wie Rollen-, Profil- und Benutzerdaten werden automatisch auf der Grundlage von Regeln festgelegt, die ebenfalls im Okta-Dienst definiert sind. So kann beispielsweise innerhalb von Okta eine Regel definiert werden, die sicherstellt, dass alle Mitglieder der AD/LDAP-Sicherheitsgruppe „Vertrieb“ ein Konto in Salesforce.com erhalten und darauf Zugriff haben.

Wenn ein Benutzer zum Verzeichnis hinzugefügt wird, werden somit alle erforderlichen Schritte für die Einrichtung des Zugriffs auf die persönliche Cloud und auf Web-Anwendungen automatisch erledigt. Dies reduziert die Bereitstellungszeit für neue Mitarbeiter erheblich und ermöglicht es IT-Administratoren, AD oder LDAP weiterhin als Ausgangspunkt für den Benutzerzugriff zu verwenden.

Wenn sich die Zugehörigkeit eines Benutzers zur Sicherheitsgruppe ändert, wird die Änderung vom Okta Directory Agent erkannt und an den Okta-Dienst weitergeleitet. In diesem Fall werden die Zuordnungsregeln erneut ausgewertet. Diese Regeln lösen entsprechende Vorgänge aus, sodass Anwendungen neu zugeordnet, bestehende Anwendungszuordnungen entfernt

oder Benutzereigenschaften in den nachgelagerten Anwendungen aktualisiert werden.

Neue und aktualisierte Anwendungszuordnungen erfolgen analog: Alle Schritte zur Bereitstellung des Kontos, zur Einrichtung von SSO und zur Aktualisierung der persönlichen Startseite „Meine Anwendungen“ werden automatisch ausgeführt. Löschungen werden ebenso behandelt: Sobald der Zugriff eines Benutzers auf eine Anwendung gelöscht wird, wird er sofort von der Verwendung von SSO für den Zugriff auf diese Anwendung ausgeschlossen. Das Anwendungskonto wird dann vom Okta-Dienst deaktiviert. Wenn dies nicht automatisch möglich ist, wird eine Admin-Aufgabe erstellt, die nach manueller Deaktivierung des Kontos abzuarbeiten ist. Alle diese Aktionen können automatisch oder nach Bestätigung durch einen Okta-Administrator ausgeführt werden.

Entzug von Berechtigungen mit nur einem Klick

Die Benutzerdeaktivierung wird typischerweise von dem standardmäßigen Identitätsspeicher wie Active Directory oder LDAP ausgelöst. Mit dem zentralen Entzug von Berechtigungen durch Okta wird sofort nach der Deaktivierung eines Benutzers im Benutzerspeicher ein entsprechender Workflow eingeleitet, um den unbefugten Zugriff auf Okta und andere Cloud-Anwendungen mit maximaler Wirkung zu gewährleisten. Der Workflow generiert eine Benachrichtigung an die Administratoren und leitet die IT-Abteilung dazu an, alle notwendigen manuellen Maßnahmen für den Entzug von Berechtigungen eines bestimmten Benutzers oder einer bestimmten Anwendung auszuführen. Darüber hinaus dient dieser Workflow auch als Audit-Trail. Innerhalb von Okta wird der gesamte Audit-Trail für Berichts- und Auditzwecke erfasst, sodass Sie problemlos Berichte über durchgeführte Maßnahmen zum Entzug von Berechtigungen nach Benutzer oder Anwendung erstellen können.

Single Sign-On für authentifizierte Anwendungen

Die meisten Unternehmen nutzen lokale Webanwendungen, die sich problemlos in die SSO-Lösung von Okta integrieren lassen. Viele Unternehmen haben auch Webanwendungen, die Verzeichnis-Anmeldedaten für die Authentifizierung verwenden. Diese Anwendungen verwenden keine integrierte Windows-Authentifizierung, sondern verlangen, dass der Benutzer beim Anmelden seine AD- oder LDAP-Anmeldedaten eingibt. Wenn Okta konfiguriert ist, um die Authentifizierung an Active Directory zu delegieren, kann die Anmeldung bei diesen internen Webanwendungen ebenfalls automatisiert werden.

Die technischen Schritte, die SSO für per Verzeichnisdienst authentifizierte interne Webanwendungen (siehe Abbildung 10) aktivieren, sind folgende:

1. **Okta ist konfiguriert, um die Authentifizierung an AD/LDAP zu delegieren.**
2. **Der Kunde verfügt über Anwendungen vor Ort, die Benutzer per AD/LDAP authentifizieren.**
3. **Der Benutzer meldet sich bei Okta mit AD/LDAP-Anmeldedaten an.**
4. **Der Benutzer greift mit SWA (Secure Web Authentication) über die AD/LDAP-Anmeldedaten auf Anwendung 1, Anwendung 2 usw. zu.**
5. **Anwendung 1 und Anwendung 2 authentifizieren den Benutzer anhand von AD/LDAP.**

Okta kann sein SWA-Protokoll (Secure Web Authentication) verwenden, um Benutzer automatisch bei diesen internen Webanwendungen anzumelden. Wenn eine interne Webanwendung konfiguriert ist, um die Authentifizierung an ein geeignetes Verzeichnis zu delegieren (also an die gleiche Quelle, an die Okta die Authentifizierung delegiert), erfasst Okta das AD/LDAP-Passwort des Benutzers bei der Anmeldung und setzt dieses Passwort automatisch für diesen Benutzer in allen Anwendungen ein, die auch an AD oder

LDAP delegieren. So können Benutzer einfach auf einen Link klicken, um auf diese Anwendungen zuzugreifen. Sie werden dann automatisch angemeldet.

Beachten Sie, dass Okta das AD-Passwort sicher synchronisiert. Wenn sich das Passwort später in AD ändert, wird dieses Ereignis beim Anmelden bei Okta erfasst und sofort im sicheren Passwortspeicher für diese Anwendung aktualisiert, damit der nächste Anmeldeversuch erfolgreich ist.

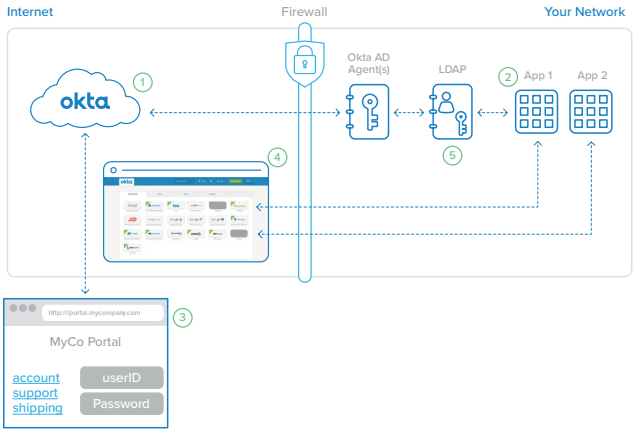

Abbildung 9: Okta ermöglicht SSO für per LDAP authentifizierte interne Webanwendungen

Fazit: Erweitern Sie Ihr Verzeichnis in die Cloud mit Okta

Unternehmen verlagern ihren Fokus zunehmend von älteren lokalen Anwendungen auf neuere Cloud-Dienste. Diese Cloud-Dienste bieten enorme Vorteile bei Funktionen und Gesamtkosten. Die Frage lautet heute nicht mehr, ob Unternehmen diese Umstellung bewerkstelligen können, sondern, wie schnell sie dies können. Eines der größten Hindernisse auf diesem Weg ist die Verwaltung von Benutzeridentitäten in einer Weise, die den Erfahrungen und Erwartungen von Benutzern und Administratoren entspricht. Die Verknüpfung von AD oder LDAP mit Cloud-Diensten löst dieses Problem – die Cloud-Lösung für das Identitätsmanagement von Okta macht es möglich. Okta bietet eine flexible, hochredundante und skalierbare Lösung für die Verwaltung von Cloud-Identitäten in Form eines Dienstes, der einfach einzurichten und praktisch wartungsfrei ist. Mit Okta können Sie Ihren zentralen Verzeichnisdienst auf alle Cloud-Anwendungen ausdehnen – auf die Anwendungen, die Sie heute nutzen, sowie auf die, die Sie in Zukunft benötigen werden.

Details zum Okta Active Directory Agent

Der AD-Agent von Okta ist einfach und transparent skalierbar. Für Redundanz kann ein Cluster erstellt werden, indem AD-Agenten auf mehreren Windows-Servern installiert werden. Der Okta-Dienst registriert jeden AD-Agenten und verteilt dann automatisch Authentifizierungs- und Benutzerverwaltungsbefehle auf sie. Wenn ein Agent die Verbindung verliert oder nicht auf Befehle reagiert, wird er aus dem Verbund entfernt und der Administrator wird per E-Mail benachrichtigt. Parallel dazu versucht der AD-Agent, sich wieder mit dem Dienst zu verbinden, indem er ein exponentielles Backoff verwendet, das auf ein Intervall von 1 Minute begrenzt ist.

Systemanforderungen für den AD-Agenten von Okta

Nachfolgend sind die minimalen Systemanforderungen zur Unterstützung des AD-Agenten von Okta aufgeführt:

- **Windows Server 2003 R2 oder höher**
- **20 MB Arbeitsspeicher für den Dienst**
- **AD-Dienstkonto, das bei der Installation des AD-Agenten von Okta erstellt wurde**

Empfohlene Systemanforderungen:

- **256 MB Arbeitsspeicher für den Dienst**
- **Eigenes AD-Dienstkonto mit Berechtigungen für Domänenbenutzer**
- **Vom Domänencontroller getrennter Server (kann gemeinsam genutzt werden)**

Details zur IWA-Webanwendung von Okta

Okta IWA ist eine IIS-Webanwendung mit geringem Ressourcenbedarf, die Desktop-SSO mit dem Okta-Dienst ermöglicht. Die Okta IWA-Webanwendung wird unter Windows Server 2008 in der Webserverrolle installiert. Das Installationsprogramm konfiguriert IIS und alle Windows-Komponenten.

Systemanforderungen für die IWA-Webanwendung von Okta

Nachfolgend sind die minimalen Systemanforderungen zur Unterstützung der IWA-Webanwendung von Okta aufgeführt:

- **Windows Server 2008 in der Webserverrolle**
- **50 MB Speicherplatz**

Details zum LDAP-Agenten von Okta

Der LDAP-Agent von Okta ist einfach und transparent skalierbar. Für Redundanz kann ein Cluster erstellt werden, indem LDAP-Agenten auf mehreren Windows-Servern installiert werden. Der Okta-Dienst registriert jeden LDAP-Agenten und verteilt dann automatisch Authentifizierungs- und Benutzerverwaltungsbefehle auf sie. Wenn ein Agent die Verbindung verliert oder nicht auf Befehle reagiert, wird er aus dem Verbund entfernt und der Administrator wird per E-Mail benachrichtigt. Parallel dazu versucht der LDAP-Agent, sich wieder mit dem Dienst zu verbinden, indem er ein exponentielles Backoff verwendet, das auf ein Intervall von 1 Minute begrenzt ist.

Systemanforderungen für den LDAP-Agenten von Okta

Nachfolgend sind die minimalen Systemanforderungen zur Unterstützung des LDAP-Agenten von Okta aufgeführt:

- **Windows Server 2003 R2 oder höher**
- **20 MB Arbeitsspeicher für den Dienst**
- **LDAP-Dienstkonto, das bei der Installation des LDAP-Agenten von Okta erstellt wurde**

Empfohlene Systemanforderungen:

- **256 MB Arbeitsspeicher für den Dienst**
- **Eigenes Dienstkonto mit Berechtigungen für Domänenbenutzer**
- **Vom Domänencontroller getrennter Server (kann gemeinsam genutzt werden)**

Der LDAP-Agent von Okta unterstützt viele der gängigen LDAP-Anbieter, darunter die folgenden:

- **SunOne LDAP 5.2+, 6.x, 7.x**
- **Oracle Internet Directory**
- **OpenLDAP**
- **OpenDJ**

Über Okta

Okta ist die Grundlage für sichere Verbindungen zwischen Mensch und Technologie. Mithilfe der Cloud gibt Okta Benutzern die Möglichkeit, jederzeit und auf jedem Gerät auf Anwendungen zuzugreifen, gleichzeitig werden strenge Sicherheitsrichtlinien durchgesetzt.
Die Lösung kann in die bestehende Verzeichnisse und Identitätsmanagementsysteme eines Unternehmens sowie in mehr als 6.000 Anwendungen direkt integriert werden.
Da Okta auf einer integrierten Plattform ausgeführt wird, können Unternehmen den Dienst schnell in großem Umfang und zu niedrigen Gesamtkosten implementieren.
Mehr als 7.000 Kunden, darunter Adobe, Allergan, Chiquita, LinkedIn, MGM Resorts International und Western Union, vertrauen auf Okta, um schneller zu arbeiten, ihren Umsatz zu steigern und ihre Sicherheit zu wahren.

Weitere Informationen finden Sie unter www.okta.com.
Folgen Sie uns außerdem unter www.okta.com/blog.