Sicherheit von Workstation-Integrationen

Kurzübersicht

Workstation verwendet beim Verbinden einer Integration zwei Arten von gesicherten Standards:

1. API-Schlüssel – gleiche Berechtigungsstufe für alle Benutzer der Anwendung. Die Integration wird standardmäßig automatisch verbunden, nachdem der Administrator sie in der Konsole aktiviert hat.
2. OAuth2.0 – Berechtigungsstufe entsprechend der Berechtigung des Benutzers in der tatsächlich verbundenen Anwendung. Die Integration erfordert die Zustimmung des Benutzers (verbinden Sie die App manuell), nachdem der Administrator sie in der Konsole aktiviert hat.

Was ist OAuth2.0

OAuth 2.0 ist ein gesicherter Datenaustauschstandard. Dieser Authentifizierungs- und Autorisierungsstandard schützt Benutzerdaten, indem er Zugriff auf die Daten gewährt, ohne die Identität oder Anmeldeinformationen des Benutzers preiszugeben. Damit kann Workstation Daten anfordern, die in der Unternehmenssuche und den Startbildschirm-Widgets angezeigt werden, ohne auf Kennwörter und andere vertrauliche Informationen zuzugreifen.

OAuth 2.0 ermöglicht es Anwendungen, auf die Daten der anderen zuzugreifen, ohne die Anmeldeinformationen des Benutzers preiszugeben. Dies erfolgt durch die Verwendung von Token, die vom Autorisierungsserver ausgestellt werden und für den Zugriff auf die geschützten Ressourcen auf dem Ressourcenserver verwendet werden können.

Sensible Daten wie Kreditkartennummern, Krankenakten, Kontoauszüge oder Passwörter werden remote gespeichert und mit einer Token-ID versehen, sodass Händler und Dritte (in diesem Fall Workstation) keinen Zugriff darauf haben.

Vorteile von OAuth 2.0

Abgesehen davon, dass das Passwort des Benutzers nicht von der Drittanbieter-Integration (in diesem Fall Workstation) preisgegeben wird, besteht einer der Hauptvorteile von OAuth 2.0 darin, dass Benutzer den Zugriff auf ihre Ressourcen jederzeit widerrufen können. Wenn Benutzer diese Drittanbieter-Integration nicht mehr benötigen, können sie einfach den Zugriff der Anwendung auf ihre Ressourcen widerrufen. Dies ist mit der herkömmlichen Benutzernamen- und Passwortauthentifizierung nicht möglich, bei der der Benutzer daran denken müsste, sein Passwort zu ändern, um den Zugriff zu widerrufen.

Darüber hinaus unterstützt OAuth 2.0 verschiedene Berechtigungstypen, mit denen der Autorisierungsserver Token auf unterschiedliche Weise ausstellen kann. Diese Flexibilität ermöglicht es dem Autorisierungsserver, basierend auf den spezifischen Anforderungen des Clients und des Benutzers die sicherste Berechtigungstype auszuwählen, und nur die relevantesten Daten gemäß vordefinierten Bereichen freizugeben.

OAuth 2.0 verfügt über ein flexibles Protokoll, das auf SSL (Secure Sockets Layer) basiert, um sicherzustellen, dass Daten zwischen dem Webserver und den Browsern privat bleiben. SSL verwendet Kryptografie-Industrieprotokolle, um Daten sicher zu halten.

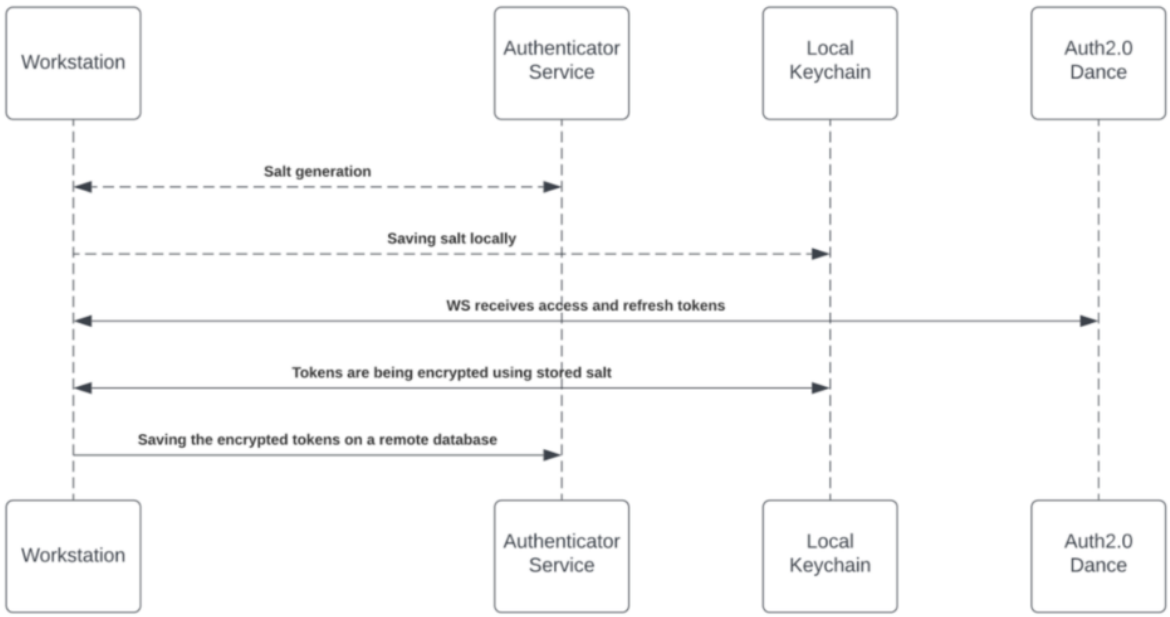
Token-Verschlüsselung aktualisieren

Immer wenn der Workstation ein neues Zugriffstoken erteilt wird, verschlüsselt die Anwendung den Zugriff und die Refresh Tokens und speichert sie in einer dezentralen Datenbank.

Der Verschlüsselungsprozess umfasst einen eindeutigen privaten Schlüssel („salt“), der für jede Person beim ersten Bootstrap generiert und in der lokalen Keychain des Computers gespeichert wird.

Das „salt“ kann nicht ersetzt oder wiederhergestellt werden – **geht es verloren, werden die Zugriffs-Token ungültig**. Diese Sicherheitsmaßnahme wird durchgeführt, um Identitäts-Spoofing beim Zugriff auf hochsensible Daten zu verhindern.

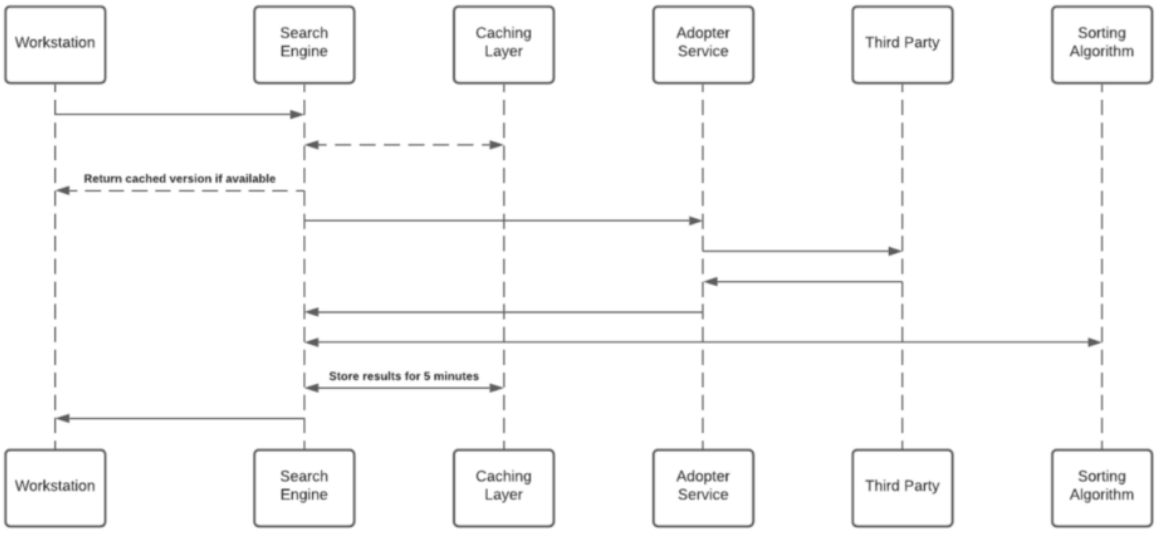
Die folgende Abbildung gibt einen Überblick, wie salt gewonnen und gespeichert wird:



Sicherheit bei der Unternehmenssuche

Die Enterprise Search verwendet Integrationen von Drittanbietern, um eine „föderale Suche“ zu implementieren. Suchvorgänge innerhalb von Workstation werden von einer NLP Engine und einer Grafikdatenbank unterstützt, die eine hervorragende Benutzererfahrung bieten.

Workstation Enterprise Search indexiert keine Daten von Drittanbietern in einer unabhängig durchsuchbaren Datenbank. Das nachfolgende Sequenzdiagramm beschreibt den Suchalgorithmus:



Cache-Layer speichert Ergebnisse für einen Zeitraum von fünf Minuten.

Jeder Adopter Service erstellt einen eindeutigen Identifikator für die Ergebnisse, der ohne Zugriff auf den Drittanbieter bedeutungslos ist und in der Grafikdatenbank gespeichert wird.

Lesen Sie mehr über die Sicherheit der Unternehmenssuche.