Open for Innovation
KNIME

KNIME Secrets Benutzerhandbuch für KNIME Community Hub

KNIME AG, Zürich, Schweiz

Version 1.16 (letzte Aktualisierung auf)

Inhaltsverzeichnis

Einleitung

Secrets bieten einen Weg, um zentral zu speichern und verwalten Logins zu anderen Systemen. Zum Beispiel a geheim könnte Anmeldeinformationen sein, um sich in eine externe Datenbank, Dateisystem oder Dienst einzuloggen. Geheimnisse werden von einem Benutzer oder einem Team-Admin verwaltet und verwaltet.

- Benutzer-Geheimnisse sind für die Verwaltung von persönlichen Logins z.B. john.smith bestimmt.
- Team-Geheimnisse auf der anderen Seite sind für geteilte Anmeldungen bestimmt, die manchmal auf als technische oder Service-Nutzer, z.B. hr_read_only, die mit mehreren Benutzern geteilt werden.

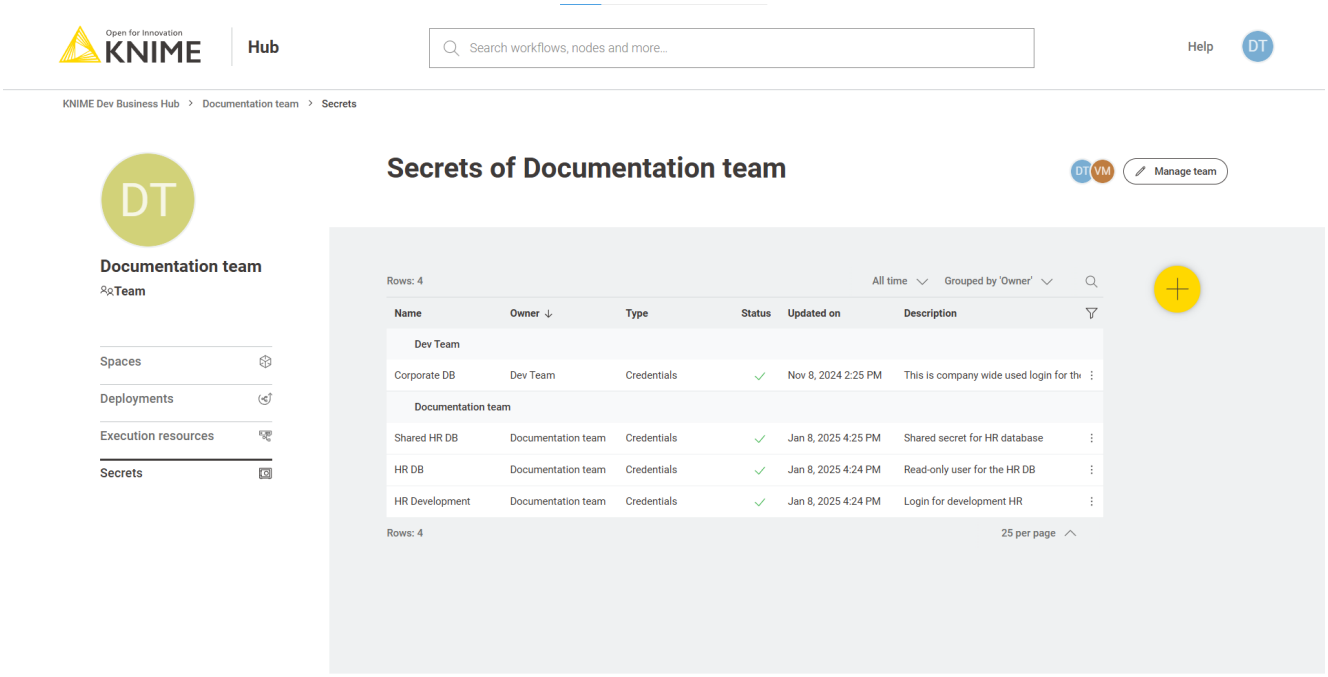
Wenn Sie auf Ihrem persönlichen kostenlosen Plan sind, können Sie nur Ihre eigenen Benutzer Geheimnisse erstellen und verwalten. Wenn Sie ein Pro-Benutzer sind, können Sie Ihre eigenen Benutzer-Geheimnisse erstellen und verwalten, entweder kostenlos Konto oder Ihr Pro-Konto. Wenn Sie ein Team-Benutzer sind, können Sie beide Benutzer erstellen und verwalten Geheimnisse und Teamgeheimnisse.

Geheimnisse verwalten

Geheimnisse werden über den KNIME Community Hub verwaltet.

- Um Ihre persönlichen Geheimnisse zu verwalten navigieren auf Ihre Kontoseite und wählen Geheimnisse aus dem Menü links. Auf deinem Geheimnisse Seite können Sie erstellen, bearbeiten und löschen persönliche Geheimnisse.
- Um Teamgeheimnisse zu verwalten, müssen Sie auf die Teamseite navigieren, die Sie verwalten möchten die Geheimnisse für. Sobald Sie auf der Teamseite sind wählen Geheimnisse aus dem Menü auf der links.

Erstellen, Bearbeiten und Löschen für persönliche, und Team-Geheimnisse funktioniert das gleiche und ist weiter unten beschrieben. Team-Geheimnisse können nur von Team-Admins erstellt werden.



Neues Geheimnis erstellen

Um ein neues Geheimnis zu erstellen, klicken Sie auf Knopf. Jedes Geheimnis besteht aus einem einzigartigen Namen, optional Beschreibung, geheimer Typ und Authentifizierungstyp. Je nach gewähltem Geheimnis und Authentifizierungstyp die zusätzlichen Eingabefelder sind unterschiedlich (für weitere Details siehe Arten Abschnitt Sobald das Geheimnis erstellt wird, ist es in der geheimen Tabelle sichtbar, die alle Geheimnisse auflisten dass Sie Zugang haben, einschließlich der, die mit Ihnen geteilt wurden.

Bearbeiten eines vorhandenen Geheimnisses

Um ein bestehendes Geheimnis zu bearbeiten, klicken Sie auf Icon in der Zeile entsprechend dem Geheimnis, das Sie wollen bearbeiten und dann klicken Bearbeiten. Dies öffnet die Menüleiste bearbeiten, wo Sie die Werte anpassen können das Geheimnis. Um die Änderungen zu speichern, klicken Sie auf Änderungen speichern Knopf. Bitte beachten Sie, dass das Geheimnis und der Authentifizierungstyp kann nicht geändert werden. Um diese zu ändern, müssen Sie ein neues erstellen geheim.

Löschen Sie ein Geheimnis

Um ein bestehendes Geheimnis zu löschen, klicken Sie auf Icon in der Zeile entsprechend dem Geheimnis, das Sie wollen um zu bearbeiten, und dann klicken löschen . Um versehentliche Löschungen zu verhindern, werden Sie aufgefordert, die Name des Geheimnisses. Sobald Sie den geheimen Namen eingegeben haben, können Sie auf die Ich verstehe die Konsequenzen, löschen Geheimnis dauerhaft um das Geheimnis zu löschen.

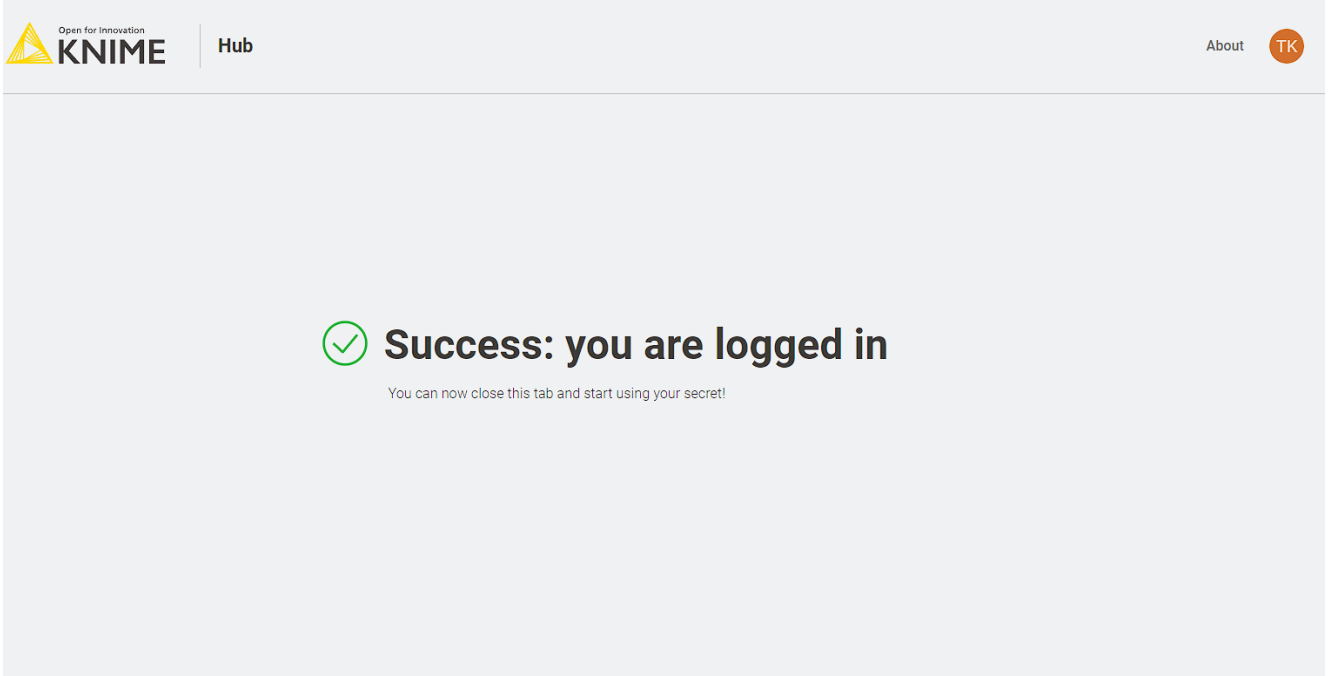
Interaktive Anmeldung

Einige Geheimnisse

und andere Geheimnisse mit interaktiven Authentifizierungstyp, verlangen, dass Sie sich in Ihr Konto einloggen, um eine Sitzung zu erwerben und zu aktualisieren token. Wenn Sie nicht eingeloggt sind, werden diese Geheimnisse in der geheimen Tabelle als Nicht Verbrauch in der Statusspalte.

Um sich anzumelden, klicken Sie auf ⋮ Icon in der Zeile entsprechend dem Geheimnis, das Sie einloggen möchten, und dann klicken Anmelden. Dies öffnet ein neues Browser-Fenster/Tab, das die Anmeldeseite der entsprechende Identitätsanbieter, z.B. Google, Microsoft, etc.

Sobald Sie eingeloggt sind, werden Sie auf die Erfolgsseite umgeleitet, die Sie schließen können.



Zugriff auf Teamgeheimnisse verwalten

Für Teamgeheimnisse können Sie wählen Zugang zur Verwaltung aus dem Menü, das beim Anklicken der ⋮ Ikone des Geheimnisses zu teilen. Dies öffnet ein Seitenpanel, wo Sie den Namen der Benutzer, mit dem Sie das Geheimnis teilen möchten. Um ein versehentliches Teilen zu verhindern, können Geheimnisse nur mit Nutzern geteilt, die Mitglieder des Teams sind.

Bei der Verwaltung des Zugangs können Sie entweder die Verwendung oder Bearbeiten Richtig. Das Nutzungsrecht erlaubt nur die Verwendung des Geheimnisses in jedem KNIME-Workflow über den Secrets Retriever-Knoten (für mehr Details siehe Verwenden von Geheimnissen Abschnitt Die Bearbeitung rechts statt, erlaubt auch den Benutzer nicht nur verwenden Sie das Geheimnis, aber auch um seine Eigenschaften zu ändern oder es zu löschen.

> Benutzer- und Pro-User-Geheimnisse können nicht mit anderen Benutzern oder Teams geteilt werden verhindern versehentliche Weitergabe von persönlichen Geheimnissen.

Best Practices für den Austausch von Geheimnissen

Wie kann ich ein Geheimnis in einer Daten-App verwenden, die ich mit anderen Benutzern teilen möchte?

Sie müssen das Geheimnis im Rahmen des Teams oder Profis erstellen, die die Daten-App bereitstellen.
Einmal erstellt, können Sie das Geheimnis in Ihrem Workflow verwenden. Der Grund dafür ist, dass die Daten-App läuft mit dem Team- oder Pro-User-Bereich, der Zugriff auf das Geheimnis hat, unabhängig davon, welcher Benutzer ist Ausführung der Daten-App.

Wie kann ich das Geheimnis des Benutzers verwenden, der die Daten-App ausführt?

Sie können die Einsteiger Widget . Dies ermöglicht es dem Benutzer, seine eigenen Anmeldeinformationen einzugeben, die sollte während der Workflow-Ausführung verwendet werden.

Verwenden von Geheimnissen

Geheimnisse können in KNIME Workflows über die Secrets Retriever Knoten. Der Knoten ist Teil von die KNIME Hub Zusätzliche Verbindung Erweiterung und muss separat installiert werden. Zu Abrufen der verfügbaren Geheimnisse der Secrets Retriever Knoten erfordert eine Verbindung zu KNIME Community Hub.

Dies kann auf zwei Arten geschehen:

ANHANG Wenn sich der Workflow in einem Raum , Sie können einfach Doppelklick auf den Workflow zu öffnen
Es. Damit wird der Workflow am Standort der KNIME Community Hub für Sie eröffnet
Nutzung durch Ihre lokale Installation des KNIME Analytics Platform Clients. Indem du das tust,
node verwendet die bestehende Verbindung zum Community Hub, um die Geheimnisse abzurufen.

2. Wenn sich der Workflow nicht auf dem Hub befindet, wird er z.B. in einem Lokaler Arbeitsraum , Sie brauchen um die KNIME Hub Authentication und verbinden Sie es mit dem Secrets Retriever Knoten über seine dynamischer Eingangsport .

Sobald der Knoten Zugang zum KNIME Community Hub hat, können Sie seinen Dialog öffnen. Im Dialog Sie können jede Anzahl von Geheimnissen auswählen, auf die Sie Zugriff haben. Je nach Art der selektiertes Geheimnis hat der Knoten verschiedene Ausgangsports z.B. eine Durchflussgröße Ausgangsport, wenn Sie Weitere Informationen zu den unterstützten Geheimtypen finden Sie in der
Geheime Typen Abschnitt.

> Aus Sicherheitsgründen werden die abgerufenen Geheimnisse nicht gespeichert, wenn der Workflow ist gespeichert. Daher muss der Knoten jedes Mal wieder ausgeführt werden, wenn ein Workflow ist geöffnet.

Während der Ausführung eines Workflows holt der Secrets Retriever-Knoten das Geheimnis aus dem Hub ab Nutzung der Rechte des Benutzers, der den Workflow ausführt. Wenn dieser Benutzer kein Recht hat, die geheim der Knoten wird scheitern Geheimnis existiert nicht Fehlermeldung.

> Secrets werden von dem Secrets Retriever-Knoten mit ihrem internen referenziert Kennung und nicht ihr Name. So ändern Sie den Namen eines Geheimnisses im KNIME Hub bricht die Verbindung nicht aus dem Secrets Retriever Knoten.

Geheime Typen

Secrets können verschiedene Arten wie Anmeldeinformationen, Zugriff auf Tokens, OAuth2 Session-Tokens oder private Schlüsseldateien. Jeder Geheimtyp kann verschiedene Authentifizierungstypen aufweisen, z.B. die Anmeldeinformationen Typ kann ein Benutzername / Passwort oder nur Authentifizierungstyp sein.

Wahl der richtigen Geheimart

Tabelle 1. Übersicht der Authentifizierungsmethoden für die Ausführung und Bereitstellung von Workflows

Interaktive und Ad-hoc-Workflow-Ausführung	**Bereitstellung von Workflows**
• Interaktives OAuth	• Dienstleistungskonten • Sicherheitstoken • Schlüsseldatei
Für ältere Systeme können Sie die Anmeldeinformationen geheimen Typ verwenden, aber es wird nicht empfohlen da jeder Benutzer mit der Erlaubnis, es zu benutzen oder Hub-Administratoren kann das Geheimnis in der Ebene anzeigen Text.	

Interaktives OAuth

Wenn Sie interaktiv mit einem Workflow in der KNIME Analytics Platform arbeiten oder diese Anzeige ausführen Hockey auf dem KNIME Hub **Interaktives OAuth** Geheimnisse.

Secret Store unterstützt derzeit interaktive OAuth für folgende Anbieter:

- Feld
- Datenbrände
- Google
- Microsoft
- <a href="#page16" style="color: #ff6600; text-decoration: underline;">

Verbesserte Sicherheit : Interaktive OAuth-Geheimnisse bieten erhöhte Sicherheit durch Multi-Faktor Authentifizierung (MFA) und Zugriff auf externe Systeme. Zusätzlich, wenn Sie interaktiver OAuth, geheimer Store stellt nur kurzlebige Session-Token aus, die generiert werden mit einem intern gespeicherten Refresh-Token, wodurch Sicherheitsrisiken weiter reduziert werden.

Einschränkungen Refresh-Tokens können ablaufen, und je nach Identitätsanbieter können Sie

müssen Einloggen erneut zu aktualisieren. Aus diesem Grund wird es nicht empfohlen, interaktive OAuth-Geheimnisse für bereitgestellte Workflows wie Datenapps oder geplante Ausführungsvorgänge. Für diese Verwendung von Fällen Servicekonten statt.

Dienstleistungskonten

Servicekonten sind eine spezielle Art von Konto, die einer Anwendung oder einer virtuellen Maschine (VM), nicht an einen einzelnen Benutzer.

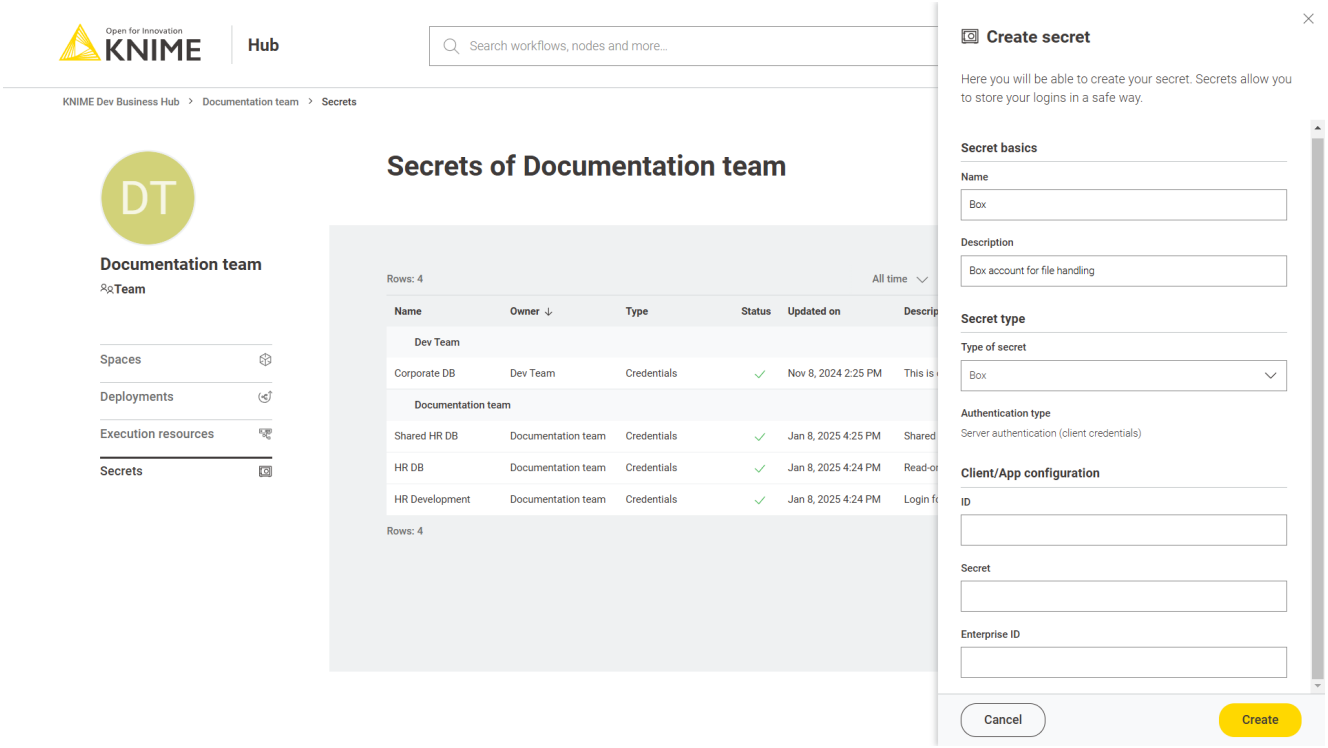
Secret Store unterstützt Servicekonten für folgende Anbieter:

- Feld
- Datenbrände
- Google
- Microsoft
- Generische OAuth-Anbieter

Wenn ein Service-Konto nicht verfügbar ist, beachten Sie die Verwendung eines Feld oder Feld. Seien Sie sich bewusst, jedoch, dass diese in der Regel den vollen Zugriff auf das externe System gewähren, so verwenden Sie sie mit Vorsicht.

> Für ältere Systeme können Sie Feld. Denken Sie daran, während KNIME versucht, Anmeldeinformationen zu verbergen, jeder Benutzer mit der Erlaubnis, ein Anmeldeinformationen geheim oder Hub-Administrator kann es in Klartext anzeigen, so dass es weniger sicher als die anderen Optionen.

Feld



Der Box-Geheimtyp ermöglicht die Verbindung zu Feld z.B. um Ihre Dateien mit der Box File Handling Extension .

Für jede der folgenden Box-Geheimtypen die Secrets Retriever node gibt ein Credential zurück <a href="#page7" style="color: #ff6600; Abschnitt Jedes Ausgabeport mit dem Box Access Token (für weitere Details siehe die selektiertes Geheimnis wird zu einem dedizierten Credential Output Port führen. Dieser Port kann als Eingang für die Box Connector Knoten, der Sie erlaubt Ihre Dateien verwalten in Box.

Benutzerauthentifizierung

Dieser Typ wird für den Benutzerauthentifizierungstyp in Box verwendet, der unterstützt OAuth 2.0 Basis Benutzerauthentifizierung.

> Dieser Authentifizierungstyp ist **nur verfügbar** für von KNIME Hubraum <a href="#page3" style="color: #ff6600; text-de <a href="#page3" style="color: #ff6600; text-de .

Dieser Typ erfordert, dass Sie sich in Box einloggen, um einen gültigen Zugriffstoken zu erhalten, bevor Sie das Geheimnis verwenden. <a href="#page4" style="color: #000000; Für Abschnitt.

Bei der Verwendung dieses geheimen Typs können Sie entweder die Standard-OAuth2-Anwendung verwenden, die von KNIME oder erstellen Sie Ihr eigenes. Um eigene zu erstellen, müssen Sie eine Individuelle App in Box.

Wenn du Einrichtung Die Box App müssen Sie die folgende hinzufügen Umleitung URI in der OAuth 2.0 Redirect URI Abschnitt in den Apps Konfiguration Seite https://api.hub.knime.com/oauth2-Strom/Kauf . Beachten Sie, dass der Hostname mit api. in der Umleitung URI. Für

mehr Details zur Einrichtung einer Benutzerauthentifizierung (OAuth 2.0) App siehe die Feld Dokumentation .

Wenn Sie Ihre eigene OAuth2-Anwendung verwenden möchten, müssen Sie die folgende angeben Autorisierung Endpunktinformation in der Erweiterte Einstellungen:

- Client/App ID: ist die Client-ID der in der OAuth 2.0 Credentials Abschnitt Ihrer App Konfiguration
- Client/App Secret: ist das Client-Geheimnis der in der OAuth 2.0 Angaben Abschnitt Ihrer App Konfiguration

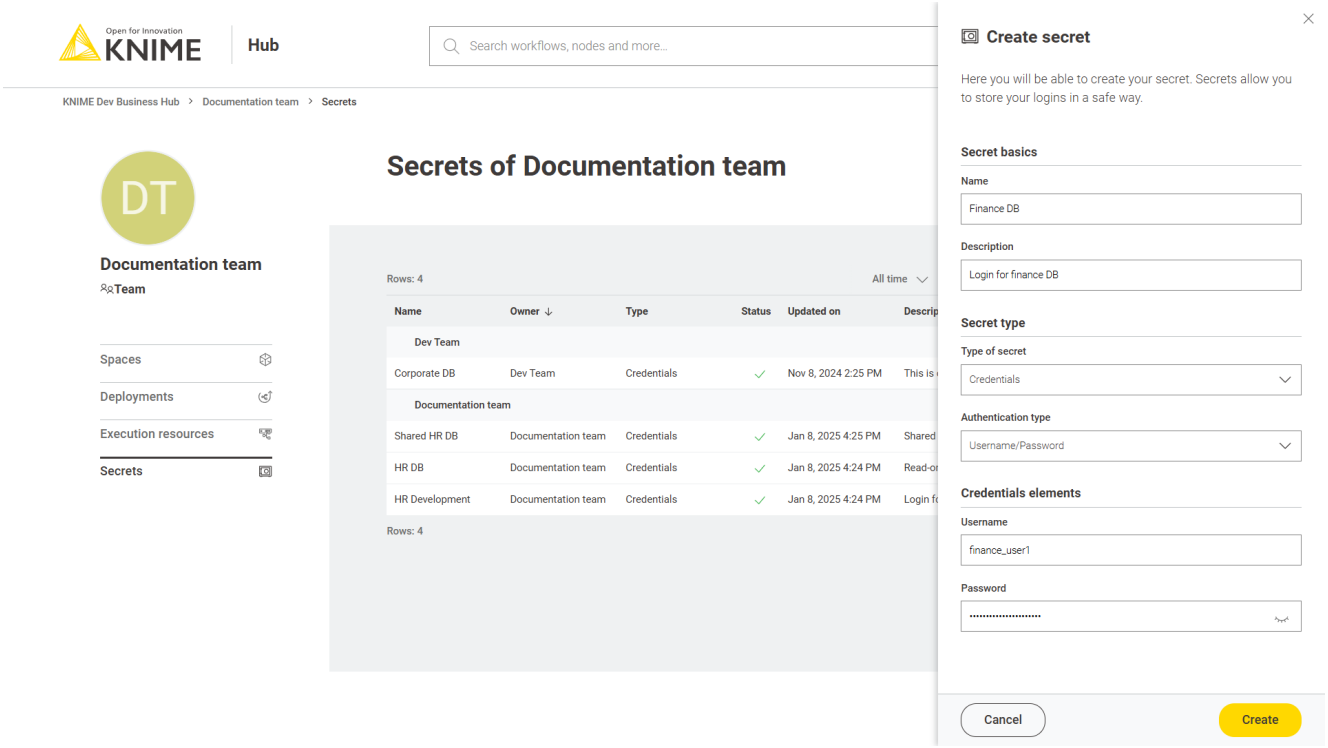
Serverauthentifizierung

Diese Art wird für die Server-Authentifizierung (Client-Berechtigungen gewähren) die empfohlen, für eingesetzte KNIME-Workflows zu verwenden. Für weitere Details zur Einrichtung einer Anwendung mit Client Credentials Grand in Box klicken Hier. .

Für diesen geheimen Typ können Sie angeben:

- Client/App ID: ist die Client-ID der in der OAuth 2.0 Credentials Abschnitt Ihrer App Konfiguration
- Client/App Secret: ist das Client-Geheimnis der in der OAuth 2.0 Angaben Abschnitt Ihrer App Konfiguration
- Enterprise ID: ist die Personalausweis wie in der Allgemeine Einstellungen Seite Ihrer App

Angaben

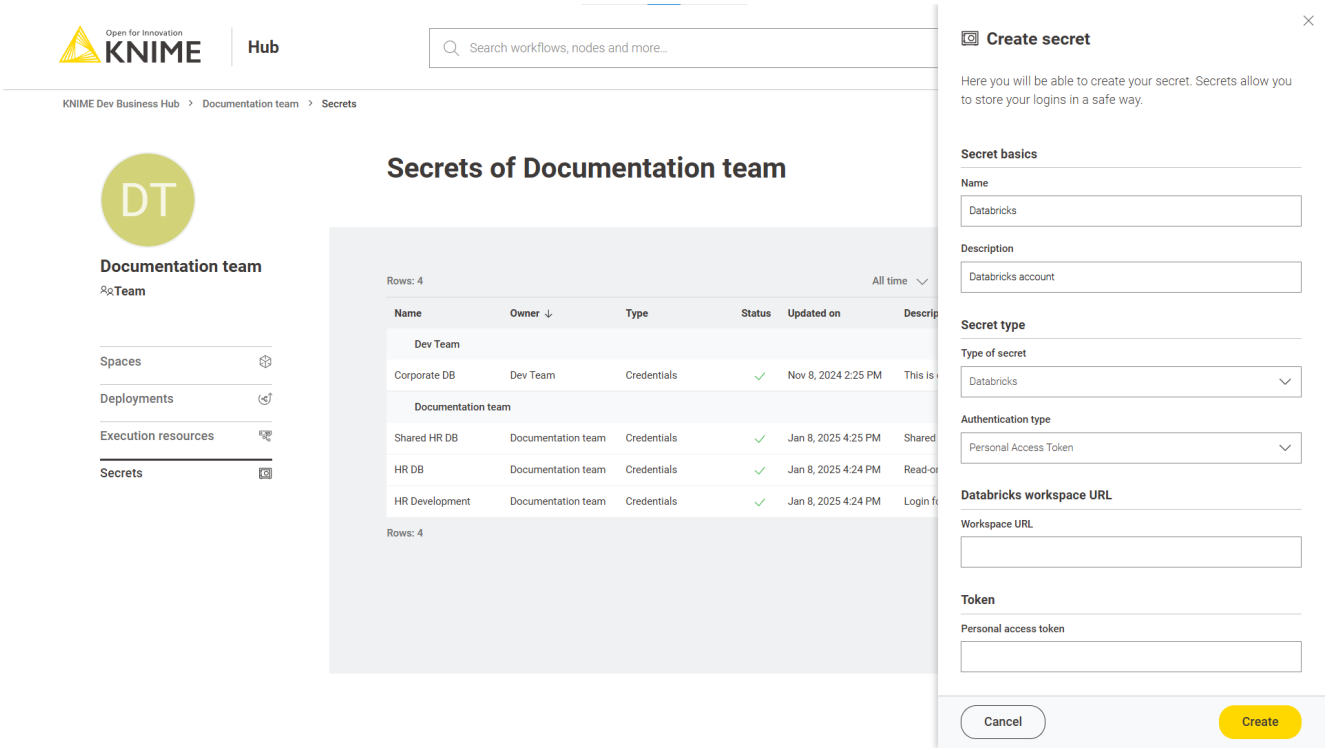


Credentials sind die grundlegendsten Arten von Geheimnissen. Sie sind in die beiden Authentifizierungen unterteilt Typen: Benutzername/Passwort und Nur noch . Wobei Benutzername/Passwort Typ Läden ein Benutzername und ein Passwort wie ein Datenbank-Login und Nur noch Typ speichert ein Passwort nur wie eine API-Taste oder Zugriffstoken.

Unabhängig von der Anzahl der ausgewählten Anmeldeinformationen geheime Typen die Secrets Retriever Knotenpunkt einen einzelnen strömungsvariablen Ausgangsport mit einer für jeden ausgewählten Anmeldestromvariablen <a href="#page7" style="color: #000000; text-decoration: none;">Abschnitt Um besser zu unterscheiden verschiedene Anmeldegrößen, Sie können den Namen für jede Variable im Knoten-Dialog angeben.

Credentials-Variablen werden von einer Vielzahl von KNIME-Knoten unterstützt, wo sie im Knoten-Dialog einem Benutzernamen und einem Passwort oder einem Token-Eingabefeld über das entsprechend Durchflussgröße Knopf.

Datenbrände



Der Databricks-Geheimtyp ermöglicht es Ihnen, verschiedene Databricks-Dienste anzuschließen, z.B. verwalten Ihre Dateien in Unity Katalog Volumen oder dirigieren Spark Jobs in der Databricks Runtime. Um diese Dienste zu nutzen, müssen Sie die KNIME Databricks Integration Erweiterung. Als Ausgangspunkt für die Arbeit mit Databricks innerhalb von KNIME siehe KNIME für Datenbrände Benutzersammlung oder KNIME Databricks Integration User Guide.

Für jede der folgenden Databricks geheime Typen die Secrets Retriever node wird zurückgeben Erstellender Ausgangsport mit dem Zugriff auf Databricks (für weitere Details siehe Geheimnisse Abschnitt Jedes ausgewählte Geheimnis wird zu einem dedizierten Credential Output Port führen. Das port kann als Eingang für die Databricks Workspace Connector der Ausgangspunkt ist um verschiedene Databricks-Dienste wie Verwaltung Ihrer Dateien in Unity Katalog Volumen Verwendung von Databricks Unity File System Connector.

Die folgenden Abschnitte beschreiben die verschiedenen unterstützten Authentifizierungstypen. Für mehr Details, auf denen die Authentifizierungsart zu wählen ist Databricks Dokumentation.

Interaktiv (OAuth2 U2M)

Dieser Typ wird zur interaktiven Authentifizierung mit Ihrem persönlichen Databricks-Login verwendet. Das Authentifizierungstyp wird auch genannt OAuth U2M oder Benutzer-zu-Maschine-Durchfluss im Datenbrände Dokumentation.

Dieser Authentifizierungstyp ist **nur verfügbar** für von KNIME Hubraum <a href="#page3" style="color: #ff6600; text-de Benutzer .

Vor der Erstellung eines interaktiven Geheimnisses müssen Sie ein App-Verbindung in Ihren Databricks Kontokonsole. Wenn Sie die Verbindung einrichten, geben Sie die folgende Umleitung URI in der URLs umleiten Abschnitt https://api.hub.knime.com/oauth2-flows/callback . In der Zugang Anwendungsbereich Wählen Sie Alle APIs . Wenn Sie die Auswahl Generieren Sie ein Client Geheimnis Option, Sie müssen Wählen Vertraulichkeit als Typ und geben Sie die Client-ID und Client-Geheimnis in das entsprechende Felder des Konfigurationsbereichs Client Ihres neuen geheimen Typs. Angemeldet bleiben Öffentliche wie Geben Sie nur die Client-ID ein. Weitere Details zum Aufbau von App-Verbindungen über die Databricks CLI oder UI sehen die Dokumentation von Databricks .

Dieser Typ erfordert, dass Sie sich bei Databricks anmelden, um ein gültiges zu erhalten Zugang zu den vor der Verwendung geheim. Für weitere Details zur Anmeldung siehe <a href="#page4" style="color: #ff6600; text-decoration Abschnitt.

Für diesen geheimen Typ können Sie angeben:

- Workspace URL: die URL der Databricks Arbeitsraum Sie wollen mitarbeiten, für Beispiel http://dbc-a1b2345c-d6e7.cloud.databricks.com
- Client-Konfigurationstyp: Wählen Vertraulichkeit wenn Sie ausgewählt haben Einen Client generieren geheimnis Option beim Erstellen App-Verbindung in Databricks. Ansonsten wählen Öffentliche.
- Client-ID: ist die Client-ID des erstellten App-Verbindung
- Client-Geheimnis: nur verfügbar, wenn Sie die Vertraulichkeit Kundentyp und nur notwendig, wenn Sie die Generieren Sie ein Client Geheimnis Option beim Erstellen Anwendung Verbindung in Databricks

Service Principal (OAuth2 M2M)

Diese Art wird für einen Databricks-Service verwendet, der empfohlen wird, für Bereitstellung von KNIME-Workflows. Dieser Authentifizierungstyp wird auch genannt OAuth M2M oder Maschine Maschinenstrom im Databricks Dokumentation. Für weitere Details zum Erstellen einer Databricks Service Hauptsächlich sehen Databricks Dokumentation.

Für diesen geheimen Typ können Sie angeben:

- Workspace URL: die URL der Databricks Arbeitsraum Sie wollen mitarbeiten, für Beispiel http://dbc-a1b2345c-d6e7.cloud.databricks.com
- Client-ID: ist die Client-ID, die wie in der Datenbrände Dokumentation
- Client-Geheimnis: ist das Geheimnis, das wie in der Datenbrände Dokumentation

Persönlicher Zugriff Token

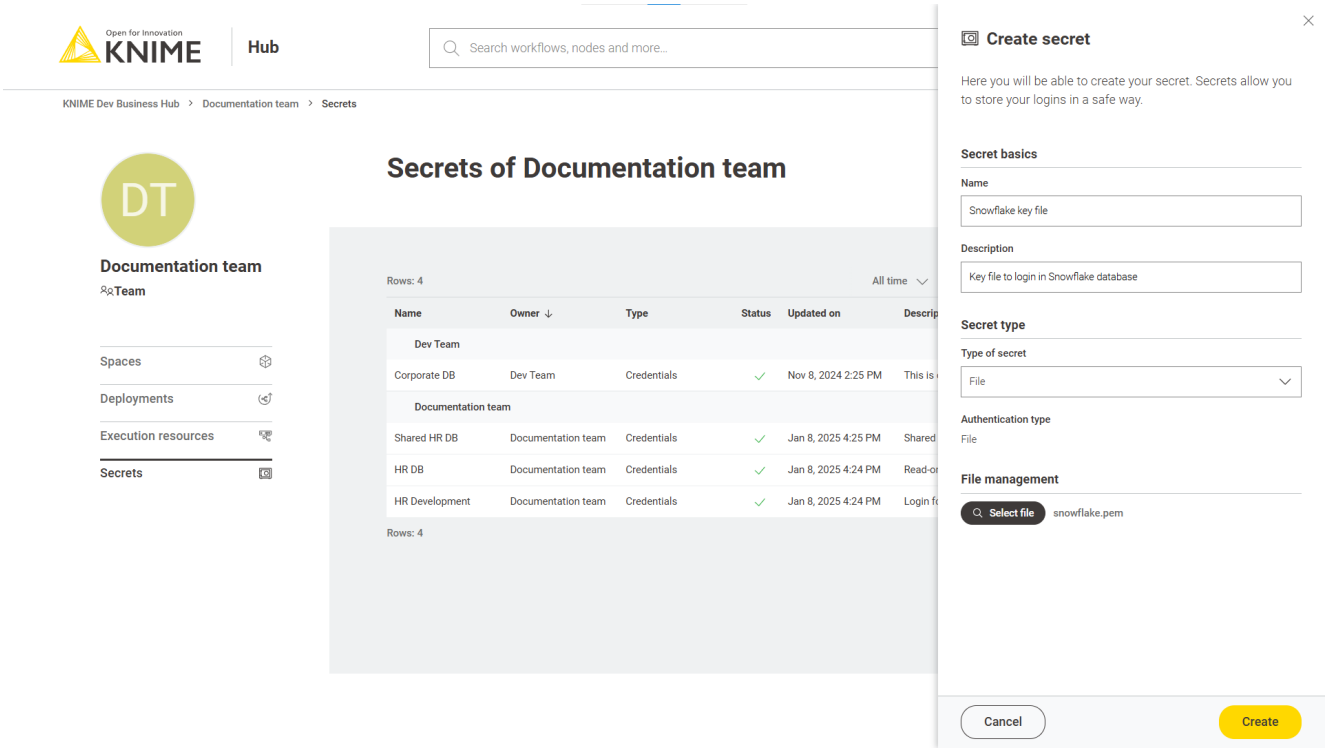
Diese Art wird für Workspace-Benutzer oder Service-Prinzips verwendet, die eine Persönlicher Zugang zu (PAT). Für weitere Informationen, wie Sie einen persönlichen Zugriff auf Token erstellen, siehe Datenbrände Dokumentation.

> Databricks empfiehlt die Verwendung von OAuth anstelle von PATs für Benutzerkonto-Client Authentifizierung und Autorisierung durch die verbesserte Sicherheit OAuth hat. Zu Verwenden Sie OAuth, wählen Sie einen der anderen Authentifizierungstypen.

Für diesen geheimen Typ können Sie angeben:

- Workspace URL: die URL der Databricks Arbeitsraum Sie wollen mitarbeiten, für Beispiel http://dbc-a1b2345c-d6e7.cloud.databricks.com
- Persönlicher Zugriffstoken: ist der wie in der Datenbrände Dokumentation

Datei



Der Dateianmeldetyp unterstützt das Speichern von beliebigen Dateien wie Api-Schlüssel oder Zertifikatsdateien mit einer maximalen Größe von 10 Kilobytes.

Unabhängig von der Anzahl der ausgewählten Datei-Geheimtypen die Secrets Retriever node wird zurückgegeben einem einzigen strömungsvariablen Ausgangsport mit Wegflussvariable für jedes ausgewählte Dateigeheimnis (für Abschnitt Um die verschiedenen Dateivariablen besser zu unterscheiden,

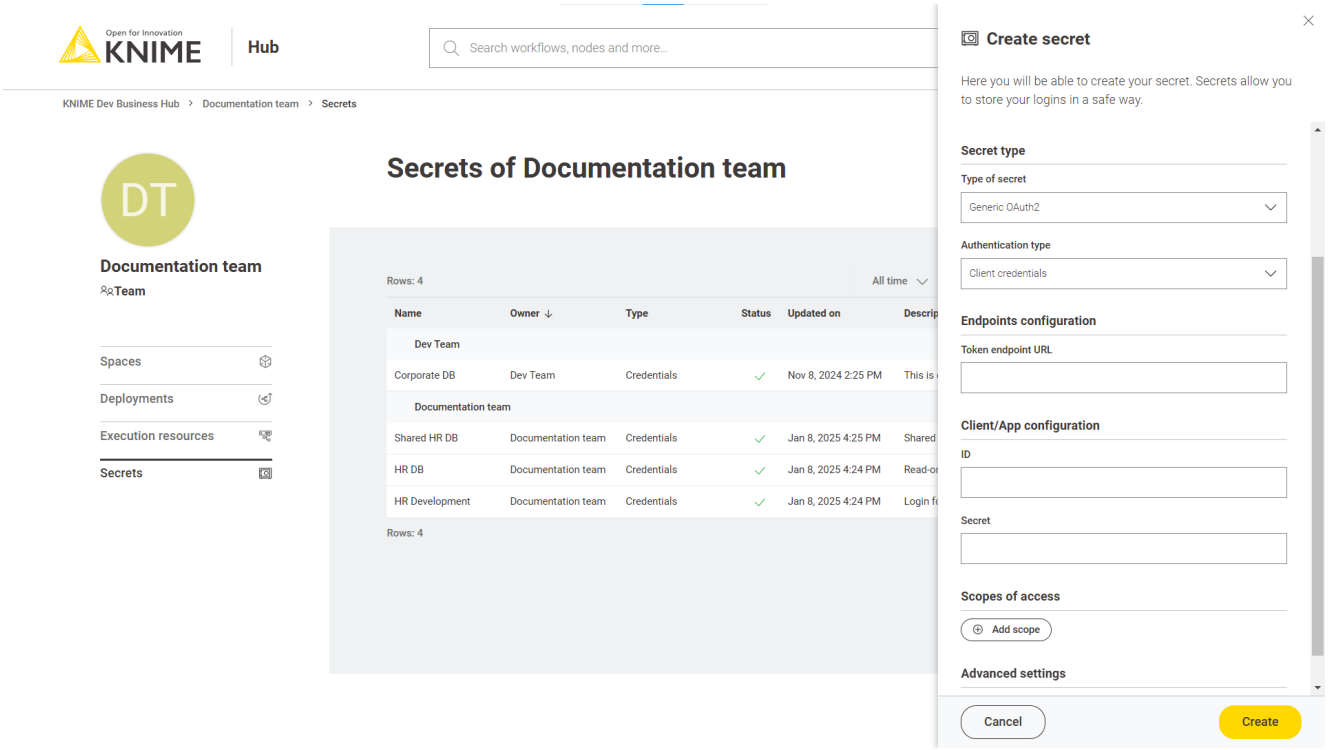
<a href="#page7" style="color:#ff6600;text-decoration:underline;">Verwenden vo

Sie können den Namen für jede Variable im Knotendialog angeben.

Path-Variablen werden von einer Vielzahl von KNIME-Knoten unterstützt, wo sie in

den Knotendialog zu einem Dateipfad über die entsprechende Durchflussgröße Knopf.

Generisches OAuth2



Der generische OAuth2 Geheimtyp ermöglicht die Verbindung zu OAuth2 konforme Authentifizierung

Anbieter, für die wir keinen speziellen geheimen Typ haben, z. Facebook, GitHub,

Instagram, LinkedIn, Slack und andere. Je nach Anwendungsfall und Erteilungsart ihr müsst

Wählen Sie einen der in den folgenden Abschnitten beschriebenen Authentifizierungstypen aus.

Für jede der folgenden allgemeinen OAuth2 geheimen Typen die Secrets Retriever node wird zurückgeben

Erstellender Ausgangsport mit dem OAuth2 Zugriffstoken (für weitere Details siehe die

Abschnitt Jedes ausgewählte Geheimnis wird zu einem dedizierten Credential Output Port führen. Dieser Hafen kann

als Eingabe für mehrere Knoten wie die REST-Knoten .

Interaktiv

Diese Art unterstützt die (interaktiv) OAuth 2.0 Zulassungscode Zuschuss. Der Auth-Code

Durch eine interaktive Anmeldung erhält man einen Zugriffstoken. Für weitere Details zur Anmeldung

in der Abschnitt.

Dieser Authentifizierungstyp ist **nur verfügbar** für von KNIME Hubraum .

Wenn Sie den Auth-Codefluss mit Ihrem Identitätsanbieter einrichten, müssen Sie Folgendes verwenden Umleitung URI: https://api.hub.knime.com/oauth2-flows/callback . Beachten Sie, dass der Hostname muss mit api. in der Umleitung URI.

Für diesen geheimen Typ können Sie angeben:

- Authorization endpoint URL: ist die Autorisierungsendpunkt-URL des OAuth-Dienstes
- Token Endpoint URL: ist die Token Endpoint URL des OAuth2 Dienstes
- Client/App-Typ: ist der Anwendungsfluss-Typ, um entweder öffentlich oder vertraulich zu verwenden
- Client/App ID: ist die Client/Anwendungs-ID manchmal API-Schlüssel genannt
- Client/App Secret: ist das Client/Anwendungsgeheimnis zu verwenden (nur für vertraulich verfügbar Typ
- Zugriffsbereich: ist die Liste der Möglichkeiten, um den Zugriff auf Token zu beantragen
- Token Endpoint Request Methode: ist die HTTP-Methode, die bei der Anforderung der Zugriff auf Token vom Token-Endpunkt
- Client/App-Authentifizierungsmethode: Gibt an, wie Client/App-ID und Geheimnis übertragen werden die Service-Endpunkte. HTTP Basic Auth ist der häufigste Mechanismus, aber einige Dienstleistungen erwarten, dass diese Werte Teil der formcodierten Anfragestelle sind.
- Verwenden Sie PKCE: wenn Sie eine Proof Key Code Exchange wird durchgeführt, was die Sicherheit

Kundeninformationen

Diese Art unterstützt die Kundenberechtigungen Zuschuss. Der Client-Anmeldezuschuss wird verwendet, um einen Zugriff auf Token im Namen eines Antrags/Kunden erhalten, ohne den Kontext eines Benutzer.

Für diesen geheimen Typ können Sie angeben:

- Token Endpoint URL: ist die Token Endpoint URL des OAuth2 Dienstes
- Client/App ID: ist die Client/Anwendungs-ID manchmal API-Schlüssel genannt
- Client/App Secret: ist das Client/Anwendungsgeheimnis zu verwenden
- Zugriffsbereich: ist die Liste der Möglichkeiten, um den Zugriff auf Token zu beantragen
- Token Endpoint Request Methode: ist die HTTP-Methode, die bei der Anforderung der Zugriff auf Token vom Token-Endpunkt

- Client/App-Authentifizierungsmethode: Gibt an, wie Client/App-ID und Geheimnis übertragen werden die Service-Endpunkte. HTTP Basic Auth ist der häufigste Mechanismus, aber einige Dienstleistungen erwarten, dass diese Werte Teil der formcodierten Anfragestelle sind.
- Zusätzliche Anforderungsfelder: sind zusätzliche Anforderungsfelder, die hinzugefügt werden sollten die token endpoint anforderung

Benutzername/Passwort

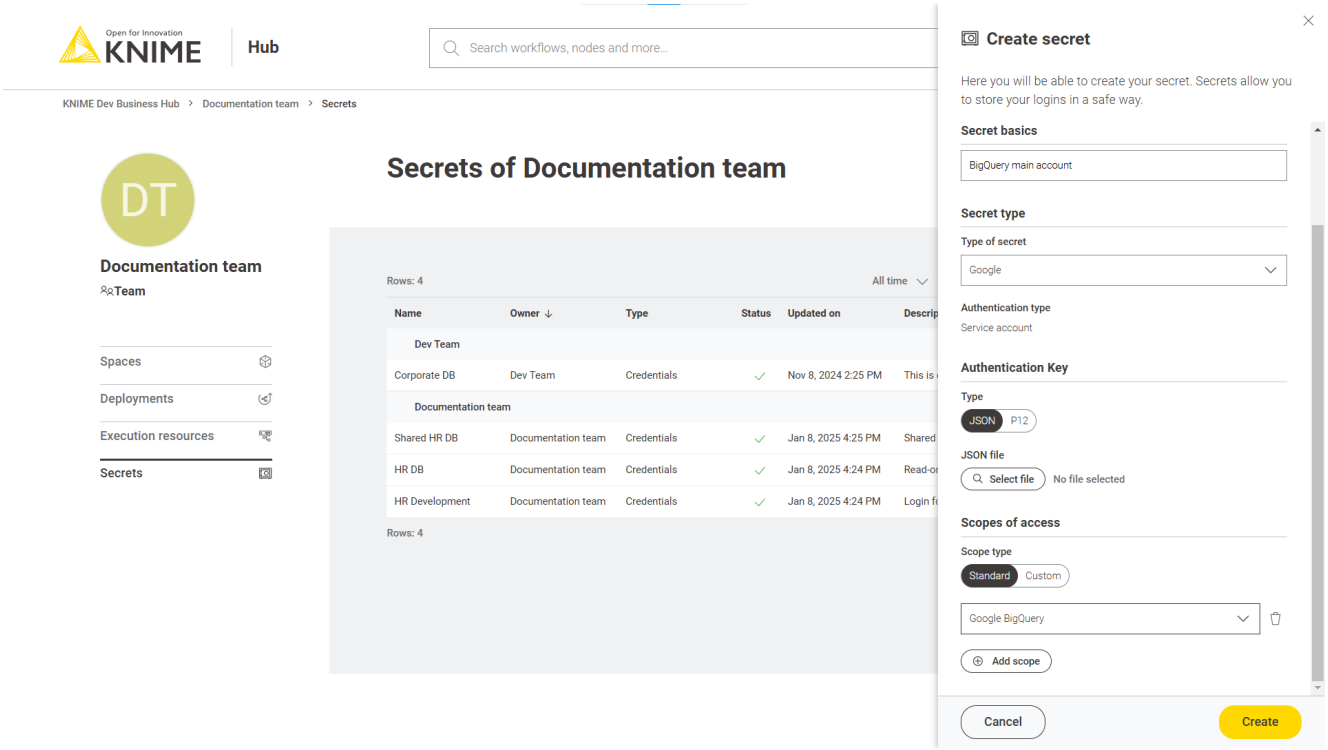
Diese Art unterstützt die OAuth 2.0 Ressourcenbesitzer Passwort-Berechtigungen (ROPC) Zuschuss.

> Der ROPC-Zuschuss gilt als veraltet und unterstützt nicht 2FA/MFA. Verwendung von Diese Zuteilung wird entmutigt und die Zuteilung der Kundenberechtigungen sollte verwendet werden statt.

Für diesen geheimen Typ können Sie angeben:

- Token Endpoint URL: ist die Token Endpoint URL des OAuth2 Dienstes
- Benutzername: ist der Benutzername zu verwenden
- Passwort: ist das Geheimnis zu verwenden
- Client/App-Typ: ist der Anwendungsfluss-Typ, um entweder öffentlich oder vertraulich zu verwenden
- Client/App ID: ist die Client/Anwendungs-ID manchmal API-Schlüssel genannt
- Client/App Secret: ist das Client/Anwendungsgeheimnis zu verwenden (nur für vertraulich verfügbar Typ
- Zugriffsbereich: ist die Liste der Möglichkeiten, um den Zugriff auf Token zu beantragen
- Token Endpoint Request Methode: ist die HTTP-Methode, die bei der Anforderung der Zugriff auf Token vom Token-Endpunkt
- Client/App-Authentifizierungsmethode: Gibt an, wie Client/App-ID und Geheimnis übertragen werden die Service-Endpunkte. HTTP Basic Auth ist der häufigste Mechanismus, aber einige Dienstleistungen erwarten, dass diese Werte Teil der formcodierten Anfragestelle sind.

Google



Der Google-Geheimtyp ermöglicht es Ihnen, verschiedene Google-Dienste zu verbinden, z.B. verwalten Sie Ihre Dateien in Google Drive über die Google Connectors Extension oder Google Cloud-Speicher Verwendung von Google Cloud-Speichererweiterung sowie die Arbeit mit Ihren Daten Google BigQuery Verwendung die BigQuery Extension.

Für jeden der folgenden Google-Geheimtypen die Secrets Retriever node wird zurückgegeben Erstellender Ausgangsport mit dem Zugriff auf Google (für weitere Details siehe Abschnitt Jedes ausgewähltes Geheimnis wird zu einem dedizierten Credential Output Port führen. Dieser Hafen kann als Eingabe für verschiedene Knoten wie die Google Driver Connector die Ihnen erlaubt Ihre Dateien verwalten in Google Drive oder Google BigQuery Connector die erlaubt, Verwaltung Ihre Daten in Google BigQuery.

<a href="#page7" style="

Interaktiv

Dieser Typ wird zur interaktiven Authentifizierung mit Ihrem persönlichen Google-Login verwendet.

Dieser Authentifizierungstyp ist **nur verfügbar** für von KNIME Hubraum .

<a href="#page3" style="color: #ff6600; text-de
Benutzerhandbuch

Vor der Erstellung eines interaktiven Geheimnisses müssen Sie ein OAuth Zustimmung Bildschirm und OAuthentizität Kunden-ID Typ Web Anwendung. Wenn Sie die Web-Anwendung einrichten, müssen Sie nicht in der Autorisierte JavaScript-Ursprünge Abschnitt. Aber du musst die ANHANG Umleitung URI in der Genehmigte Umleitung URIs Abschnitt in der Oauth Client ID Seite https://api.hub.knime.com/oauth2-flows/callback . Für weitere Details

über die Authentifizierung im Allgemeinen und weitere Details, wie Sie den OAuth-Einwilligungsbildschirm einrichten und Client-ID sehen Google-Dokumentation .

Dieser Typ erfordert, dass Sie sich bei Google anmelden, um ein gültiges zu erhalten Zugang zu den vor der Verwendung des Geheimnisses.

<a href="#page4" style="color: #000000; text-decoration: underline;">Abschnitt.

Für diesen geheimen Typ können Sie angeben:

- Client/App ID-Datei: ist die OAuth Client ID geheime Datei (zum Beispiel Datei klicken) Hier.)
- Zugriffsumfang: sind die Möglichkeiten, die Sie während des Logins anfordern können (für weitere Details siehe die <a href="#page20" style="color: #ff6600; text-decoration: underline;">OAuth2 Anwendungsbereic Abschnitt

Servicekonto

Diese Art wird für eine Servicekonto die für die Bereitstellung von KNIME empfohlen wird Workflows. Für weitere Details zur Einrichtung eines Service-Accounts in Google klicken Hier. .

Für diesen geheimen Typ können Sie angeben:

- Authentication Schlüsseltyp: ist entweder JSON (empfohlen) oder P12 Format
- JSON oder P12-Datei: Je nach gewähltem Schlüsseltyp laden Sie entweder Ihren JSON hoch oder P12 Schlüsseldatei(Siehe die Google-Dokumentation wie man eins erstellt)
- Service-Account-E-Mail: ist die E-Mail-Adresse des Service-Accounts (nur verfügbar für Typ P12
- Zugriffsumfang: sind die Möglichkeiten, die Sie während des Logins anfordern können (für weitere Details siehe die <a href="#page20" style="color: #ff6600; text-decoration: underline;">OAuth2 Anwendungsbereic Abschnitt

Standard OAuth2 Bereiche für Google-Dienste

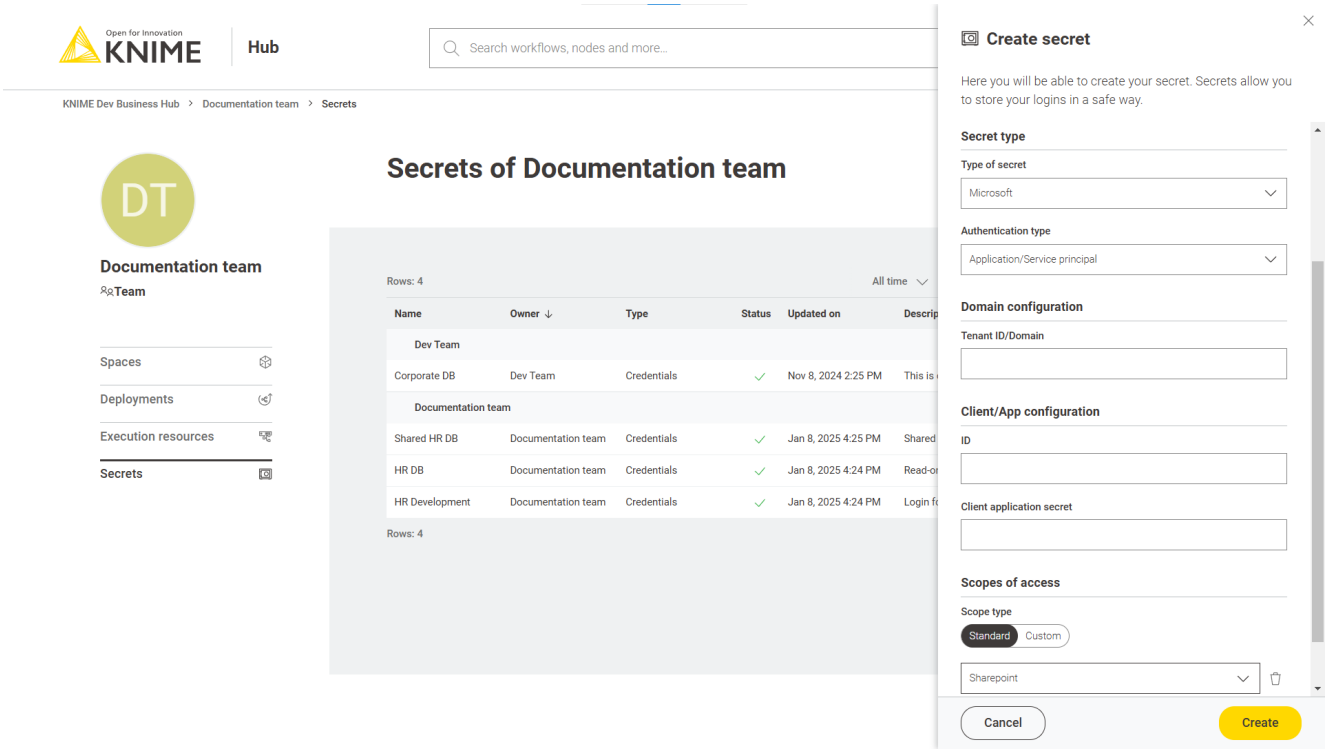
Dieser Abschnitt listet die verschiedenen Bereiche für die häufigsten Google-Dienste, auf die Sie zugreifen können aus der KNIME Analytics Platform.

Für weitere Details und eine vollständige Liste aller verfügbaren Bereiche siehe die Google Dokumentation . Um eines der unten genannten gemeinsamen Dienste zu nutzen, kopieren Sie die URL neben den Service und fügen Sie ihn in die Geltungsbereich des Zugangs Teil des Geheimnisses.

- Google Analytics (nur lesen): http://www.googleapis.com/auth/analytics.readonly
- Google BigQuery: http://www.googleapis.com/auth/bigquery
- Google Drive (nur lesen): http://www.googleapis.com/auth/drive.

- Google Drive: https://www.googleapis.com/auth/drive
- Google Sheets (nur lesen): https://www.googleapis.com/auth/spreadsheets.readonly und http://www.googleapis.com/auth/drive.readonly
- Google Sheets: https://www.googleapis.com/auth/spreadsheets und http://www.googleapis.com/auth/drive.

Microsoft



Die Microsoft-Geheimtypen ermöglichen es Ihnen, mit der Microsoft/Azure-Cloud-Plattform zu verbinden Knoten aus folgenden Erweiterungen:

- KNIME Office 365 Connectors
- KNIME News und News
- KNIME Azure Cloud Connectors
- KNIME Integration von BI
- KNIME Integration von Snowflake
- KNIME Datenbank (Microsoft SQL Server Connector Knoten
- KNIME REST Client Erweiterung

Für jeden der folgenden geheimen Typen wird der Secrets Retriever-Knoten ein Credential zurückgeben Ausgangsport, der entweder einen OAuth2-Zugangstoken oder einen Azure-Speicher-Anmeldedaten enthält (für

Abschnitt Jedes ausgewählte Geheimnis wird zu einem eigenen Ergebnis führen

Credential Output Port. Dieser Port kann als Eingabe für Knoten aus den obigen Erweiterungen verwendet werden.

Interaktiv

Dieser Typ unterstützt einen interaktiven Login in der Microsoft/Azure Cloud mit Ihrem Microsoft Identität.

Dieser Authentifizierungstyp ist **nur verfügbar** für von KNIME Hubraum .

token. Beachten Sie, dass irgendwann die Anmeldung abläuft und ein neues Login erforderlich ist, daher dies geheime Art ist nicht für geplante oder anderweitig automatisierte Workflows auf KNIME geeignet Hub.

einen gültigen Zugriff erhalten

Um das Geheimnis zu konfigurieren, können Sie entweder die von KNIME bereitgestellte App nutzen oder sich selbst registrieren. App in Azure Entra ID (früher Azure Active Directory) muss registriert werden (siehe Abschnitt

Wenn Sie Ihre eigenen App, die Sie benötigen, um die folgenden Berechtigung Endpoint-Informationen anzugeben in den erweiterten Einstellungen:

- Client/App-Konfiguration:

  ANHANG Wählen Sie:

  a. Öffentlichewenn Sie eine ÖffentlicheApp in Azure Entra ID. Das bedeutet, dass Sie ausgewählt Public Client/native (Mobile & Desktop) unter Redirect URI wenn .

  B. Vertraulichkeit wenn Sie eine Vertraulichkeit App in Azure Entra ID. Das bedeutet, dass Sie ausgewählt haben Web unter Redirect URI wenn .

  2. Geben Sie die Anwendungs-ID der zuvor registrierten Azure App ein

- Zugriffsbereich: Geben Sie eine Liste von Bereichen ein, die das resultierende Geheimnis begrenzen können verwendet, um z.B. nur auf SharePoint zuzugreifen; während des interaktiven Logins müssen Sie möglicherweise Zustimmung zu den beantragten Bereichen (für weitere Details siehe Abschnitt

- Authorization Endpoint: Verwenden Sie entweder die Standard-URL oder geben Sie eine benutzerdefinierte ein, die erlaubt zu einem bestimmten Azure-Tenant unterschreiben

Die Anmeldung basiert auf der OAuth 2.0 Zulassungscode fließen.
Mit dem interaktiven Login kann KNIME Hub temporären Zugriff erhalten und speichern
und aktualisieren Sie die Token im Auftrag des Benutzers. KNIME Hub erfrischt und kehrt zurück
erwarb Zugriffstoken, wenn das Geheimnis in einem Workflow verwendet wird. Die ausgewählte
Umfange entsprechen delegierte Berechtigungen in Microsoft/Azure. Beraten Sie die
für weitere Informationen zur korrekten Einrichtung einer Azure
App.

Anmeldung/Dienstleistung

Diese Art unterstützt die Authentisierung als Anwendungs- oder Service-Prinzip in der
Microsoft/Azure Cloud. Dies ist gut für geplante oder anderweitig automatisierte Workflows geeignet
auf KNIME Hub, wo kein Benutzer zur interaktiven Anmeldung anwesend ist.

Voraussetzung für eine App in Azure Entra ID (früher Azure Active Directory) muss sein
.

Für diesen geheimen Typ können Sie angeben:

- Domain-Konfiguration: Geben Sie den Azure-Tenant zum Zugriff an, entweder im ID-Format, z.
  faa16e7e-a95d-4117-b2c7-06ffc6e68acb , oder als Domain-Name, z.
  contoso.com
- Client ID und Geheimnis: Geben Sie die Client-ID und das Geheimnis der zuvor registrierten Azure ein
  Anwendung
- Zugriffsbereich: Geben Sie eine Liste von Bereichen ein, die das resultierende Geheimnis begrenzen können
  verwendet, um z.B. nur auf SharePoint zuzugreifen (für weitere Details siehe die
  Abschnitt

Die Authentifizierung basiert technisch auf der OAuth 2.0 Client
Angaben fließen. KNIME Hub fordert einen neuen Zutritt, wenn das Geheimnis
wird in einem Workflow verwendet. Die ausgewählten Anwendungsbereiche entsprechen Anwendungsbereich
Berechtigungen in Microsoft/Azure. Konsultieren Sie das jeweilige für mehr
Informationen zur korrekten Einrichtung einer Azure App und Anwendung
Berechtigungen.

Benutzername/Passwort

Dieser Typ unterstützt die Authentisierung als Benutzer in der Microsoft/Azure Cloud. Es kann für
geplante oder anderweitig automatisierte Workflows am KNIME Hub, bei denen kein Benutzer anwesend ist,
interaktiv einloggen. Beachten Sie jedoch, dass dieser Authentifizierungstyp entmutigt von Microsoft . Es

unterstützt die Konten 2FA/MFA nicht und hat weitere Einschränkungen.

Voraussetzung für eine App in Azure Entra ID (früher Azure Active Directory) muss sein registriert. Bitte sehen Sie die jeweiligen Wie man .

Für diesen geheimen Typ können Sie angeben:

- Credentials: Geben Sie Ihren Microsoft/azure Benutzernamen und Ihr Passwort an.
- Client/App-Konfiguration: Geben Sie die Client-ID der zuvor registrierten Azure App ein
- Zugriffsumfang: Geben Sie eine Liste von Bereichen ein, um zu begrenzen, was das resultierende Geheimnis verwendet werden kann z.B. nur auf SharePoint zugreifen (für weitere Details siehe die <a href="#page25" style="color: #ff66 Abschnitt
- Authorization Endpoint: Verwenden Sie entweder die Standard-URL oder geben Sie eine benutzerdefinierte ein, die erlaubt zu einem bestimmten Azure-Tenant unterschreiben

> Die Authentifizierung basiert technisch auf der OAuth 2.0 Ressourcen Owner Password Credentials Flow. KNIME Hub fordert einen neuen Zugriff auf wenn das Geheimnis in einem Workflow verwendet wird. Die ausgewählten Anwendungsbereiche entsprechen delegierte Berechtigungen in Microsoft/Azure. Konsultieren Sie das jeweilige Wie man für mehr Informationen über die korrekte Einrichtung einer Azure App und delegierter Berechtigungen.

Azure Storage freigegebene Zugriffssignatur (SAS)

Diese Art ermöglicht die Authentifizierung gegen Azure Blob Storage/Data Lake Storage Gen2 mit einem Gemeinsame Zugangsunterschrift (SAS) . Ein SAS gewährt eingeschränkten und zeitlich begrenzten Zugang zu einem Azure Aufbewahrungsbehälter oder Gegenstände innerhalb. Vgl. Hier. für weitere Dokumentationen.

Für diesen geheimen Typ müssen Sie nur eine SAS URL angeben. Konsultieren Sie das jeweilige <a href="#page33" style für wie man eine SAS-URL erstellt.

Azure Storage geteilter Schlüssel

Diese Art ermöglicht die Authentifizierung gegen Azure Blob Storage/Data Lake Storage Gen2 mit einem geteilter SchlüsselDer gemeinsame Schlüssel gewährt uneingeschränkten Zugang zu einem Azure Storage-Konto und alle Container innerhalb. Vgl. Hier. für weitere Dokumentationen.

> Microsoft/Azure empfiehlt, keine gemeinsame Schlüsselauthentifizierung zu verwenden, da es bietet uneingeschränkten Zugriff auf ein Azure Storage-Konto und alle Container innerhalb. Alle anderen Authentifizierungstypen in diesem Abschnitt können verwendet werden statt.

Für diesen geheimen Typ müssen Sie angeben:

- Speicherkonto: Geben Sie den eindeutigen Namen des Speicherkontos ein
- Geteilter Schlüssel: der geteilte Schlüssel, der sich wie beschrieben befinden kann

<a href="#page34" style="color: #f

Standard OAuth2 Bereiche für Azure-Dienste

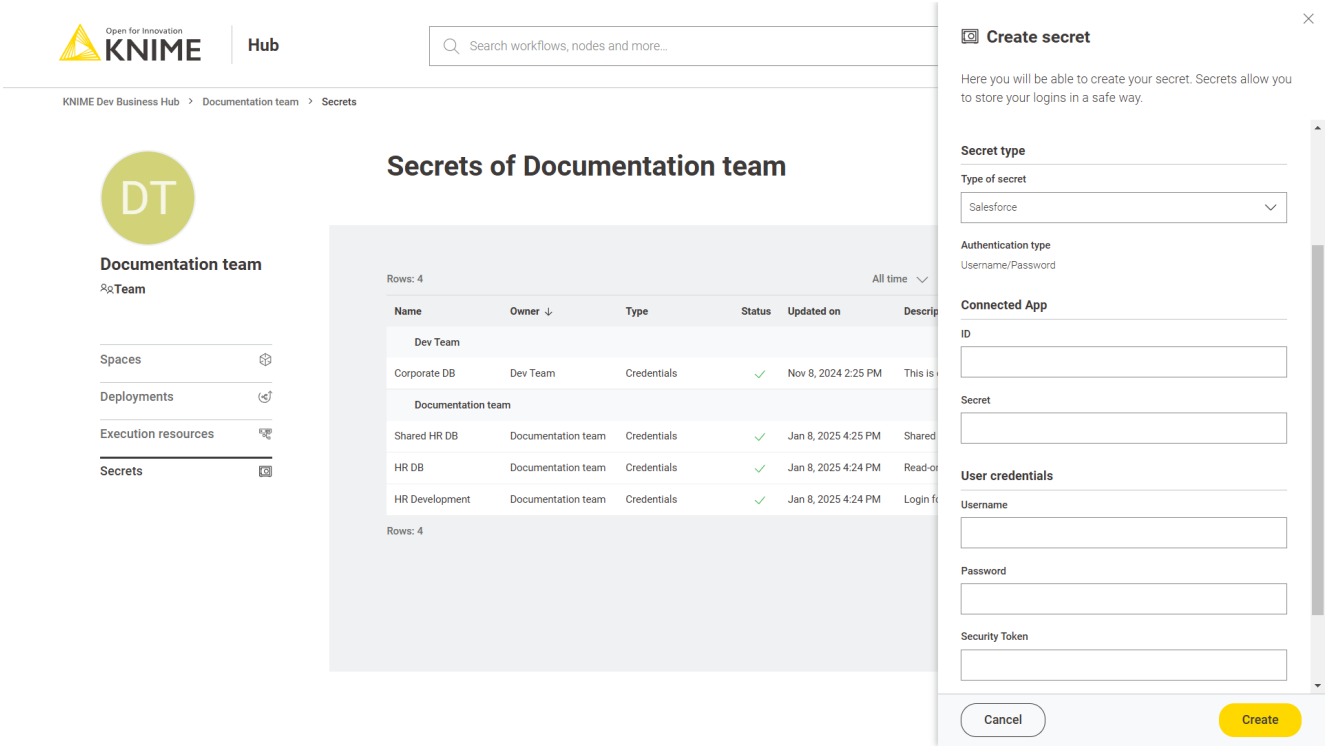
Dieser Abschnitt listet die verschiedenen Bereiche für die häufigsten Azure-Dienste, die Sie von innerhalb der KNIME Analytics Platform. Für weitere Details und eine vollständige Liste aller verfügbaren Die Microsoft-Dokumentation . Zur Nutzung eines der genannten gemeinsamen Dienste unter Kopieren Sie den Umfang neben dem Dienst und fügen Sie ihn in die Geltungsbereich des Zugangs Abschnitt der geheim.

- Sharepoint-Dateien und Listenartikel (Lesen Sie): Sites. Lesen.All Diese Berechtigung erlaubt das Token zum Lesen von Dateien und Listendateien, die auf SharePoint Online gespeichert werden. Hinweis: Zugriff auf jede bestimmte SharePoint-Website muss zusätzlich dem Benutzer von dieser Seite gewährt werden.
- Sharepoint-Dateien und Listenartikel (Read/Write): Sites. ReadWrite. Alle Diese Erlaubnis ermöglicht es dem Token, Dateien zu lesen und zu schreiben sowie Listen-Elemente auf SharePoint gespeichert Online. Dies beinhaltet das Erstellen und Löschen von Dateien, aber nicht Listen. Beachten Sie, dass der Zugriff auf alle spezifische SharePoint-Website muss dem Benutzer zusätzlich von dieser Website gewährt werden.
- Sharepoint-Dateien, Listen und Listenelemente (Read/Write): Seiten.Verwalten. Alle Diese Erlaubnis ermöglicht es dem Token, Dateien, Listen sowie Listendateien zu lesen und zu schreiben, die auf SharePoint gespeichert sind Online. Dies beinhaltet das Erstellen und Löschen von Dateien sowie Listen. Beachten Sie, dass der Zugriff auf alle spezifische SharePoint-Website muss dem Benutzer zusätzlich von dieser Website gewährt werden.
- Benutzergruppen (Lesen) (Erfordert Admin-Einwilligung): Verzeichnis.Read.All Diese Erlaubnis ist erforderlich, um die Office 365 Gruppen, die der eingeloggte Benutzer ist ein Mitglied von, wenn Wählen Sie eine SharePoint-Team-Website, um sich anzuschließen. Beachten Sie, dass diese Erlaubnis nur von einem Entra-ID-Admin.
- Benutzergruppen (Lesen) (Limited): Benutzer.Lesen Diese Berechtigung ist erforderlich, um die Office 365 Gruppen, die der eingeloggte Benutzer ein Mitglied ist, bei der Auswahl eines SharePoint Team-Website zu verbinden. Diese Erlaubnis erfordert keine Zustimmung durch einen Administrator, aber nicht auf die human lesbaren Namen von Office 365 Gruppen zugreifen können, daher nur technische IDs werden angezeigt.
- Azure Blob Storage/Azur Daten Lake Storage Gen2: Bitten Sie die User imperson Erlaubnis für ein bestimmtes Azure-Speicherkonto. Diese Berechtigung ermöglicht das Token Zugriffsdaten, die in diesem Speicherkonto gespeichert sind. Beachten Sie, dass der Zugriff auf bestimmte Daten in dass dem Benutzer zusätzlich ein Konto zur Verfügung gestellt werden muss, bevor ein Zugriff möglich ist.
- Azure SQL Datenbank: Fordert die User imperson Erlaubnis. Diese Erlaubnis

ermöglicht den Zugriff auf die Azure SQL API. Beachten Sie, dass der Zugang zu einem bestimmten Datenbanken/Ressourcen müssen dem Benutzer zusätzlich gewährt werden, bevor tatsächliche Zugang ist möglich.

- Power BI: Dataset. ReadWrite. Alle und Workspace.Read.All .

Umsatz



Der geheime Typ von Salesforce ermöglicht die Verbindung zu Umsatz indem die Knoten aus der Erweiterung von Salesforce .

Für jede der folgenden Salesforce-Geheimtypen die Secrets Retriever node wird zurückgeben Salesforce Credential Output Port mit dem Salesforce Access Token (für weitere Details siehe die Verwenden von Geheimnissen Abschnitt Jedes ausgewählte Geheimnis wird zu einem dedizierten Credential Output Port führen.

Dieser Port kann als Eingang für die Salesforce Connector Knoten, der der Startknoten ist Zugriff auf Ihre Daten in Salesforce.

Vor der Erstellung einer dieser geheimen Typen müssen Sie eine Vernetzte App in Salesforce mit OAuth-Einstellungen aktiviert . In der API (OAuth-Einstellungen aktivieren) Abschnitt, den Sie bereitstellen müssen Die folgende Callback URL https://api.hub.knime.com/oauth2-flows/callback . Anmerkung: der Hostname muss mit api. in der Umleitung URI. Für weitere Informationen über die OAuth Authorization Flows im Allgemeinen Dokumentation der Salesforce.

Interaktiv

Diese Art wird für die OAuth 2.0 Web Server Flow in Salesforce, die die OAuth 2.0 Autorisierungscode Grant-Typ.

> <a href="#page3" style="color: #ff6600; text-de
> Dieser Authentifizierungstyp ist **nur verfügbar** für von KNIME Hubraum
> <a href="#page3" [illegible]
> .

Diese Art erfordert, dass Sie sich bei Salesforce anmelden, um einen gültigen Zugriffstoken zu erhalten, bevor Sie die geheim. Für weitere Details zur Anmeldung siehe <a href="#page4" style="color: #ff6600; text-decoratio Abschnitt.

Für diesen geheimen Typ können Sie angeben:

- Connected App ID: ist der Verbraucherschlüssel der angeschlossenen Anwendung, der als beschrieben Hier.
- Connected App Secret: ist das Verbrauchergeheimnis der angeschlossenen Anwendung, die als beschrieben angesehen Hier.
- Salesforce-Instanz: ist der Beispieltyp Salesforce Produktion oder Sandkasten für Prüfverfahren

Benutzername/Passwort

Diese Art wird für die OAuth 2.0 Benutzername-Passwort-Durchfluss die zu verwenden ist für den Einsatz von KNIME-Workflows.

Für diesen geheimen Typ können Sie angeben:

- Connected App ID: ist der Verbraucherschlüssel der angeschlossenen Anwendung, der als beschrieben Hier.
- Connected App Secret: ist das Verbrauchergeheimnis der angeschlossenen Anwendung, die als beschrieben angesehen Hier.
- Benutzername: ist der Benutzername
- Passwort: ist das Passwort
- Security Token: ist der optionale Sicherheitstoken
- Salesforce-Instanz: ist der Beispieltyp Salesforce Produktion oder Sandkasten für Prüfverfahren

Bereiten Sie Ihre Dienste für die Nutzung mit KNIME vor Geheimnisse

Dieser Abschnitt erklärt, wie Sie externe Dienste vorbereiten, so dass ihre Anmeldeinformationen, Apps oder Schlüssel kann als Geheimnisse gespeichert und sicher in Ihren Workflows verwendet werden.

Bereiten Sie eine Azure-App für die Benutzerauthentifizierung vor

So wird beschrieben, wie man eine Azure App einrichten kann, so dass sie mit Geheimnissen des Typs verwendet werden kann
<a href="#page22" style= [illegible]
.

Voraussetzungen:

- Zulassung zur Registrierung von Apps in Azure Entra ID. Azure Admins haben in der Regel diese die Genehmigung, kann aber auch durch Rollen wie die Anwendung Administrator oder Anwendung Entwickler (siehe Hier.)

Schritte:

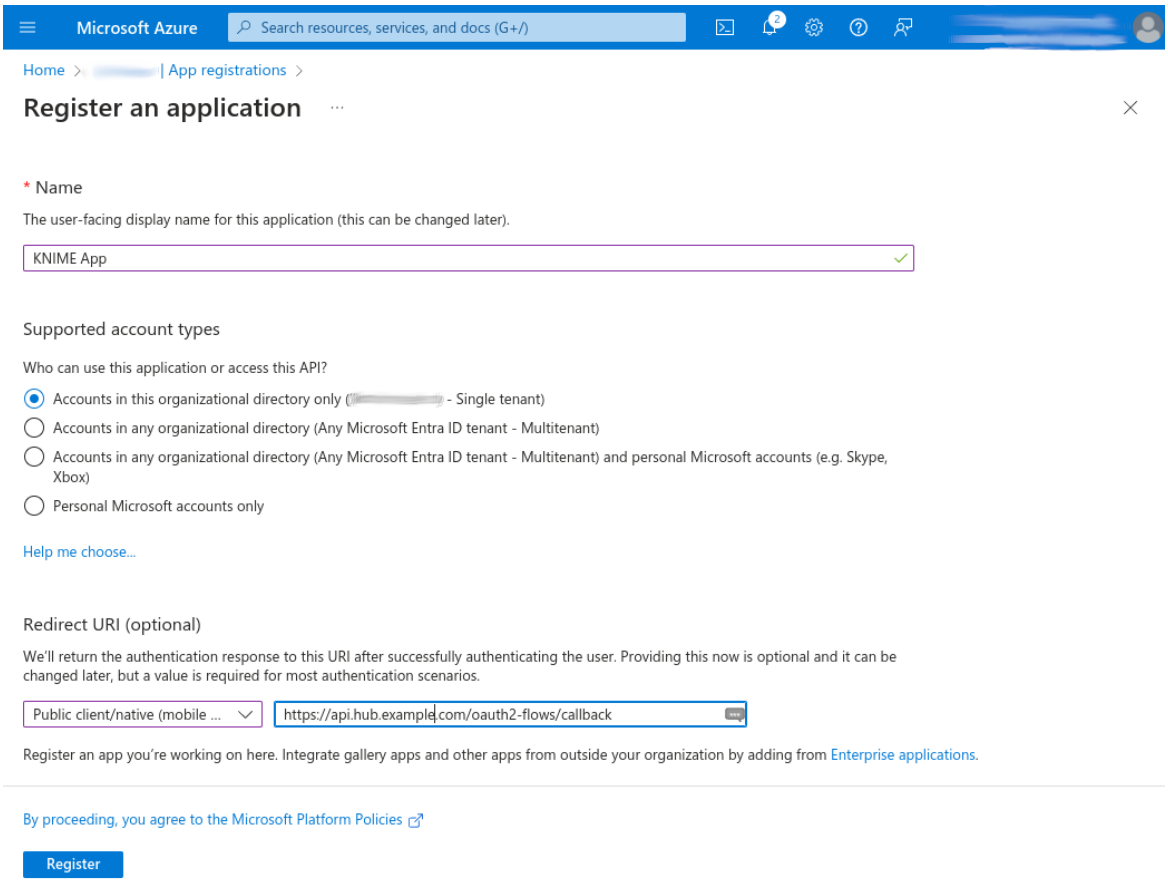
ANHANG Einloggen in die Azure Portal

2. Navigieren zu Azure Entra ID → Anmeldungen der App

3. Eine neue App registrieren:

   a. Klicken Sie auf Neue Anmeldung

   B. Geben Sie einen Namen ein und wählen Sie den unterstützten Kontotyp (Einzelmiete in den meisten Fälle



c. Unter Redirect URI :

i. Wählen Sie die aufgerufene Plattform aus:

A. Web , oder

B. Public Client/native (Mobile & Desktop)

ii. Geben Sie https://api.hub.knime.com/oauth2-flows/callback . Anmerkung:

Hostname muss mit api. in der Umleitung URI.

d. Klicken Sie auf Register

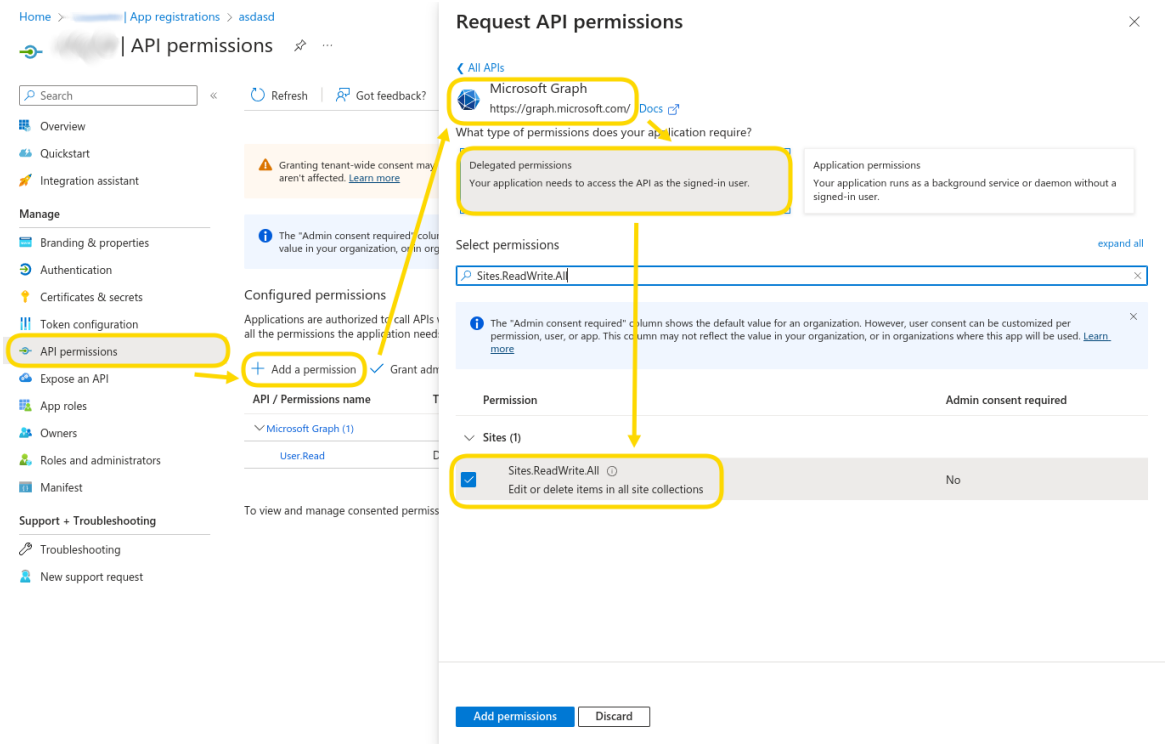
L 347 vom 20.12.2013, S. 1). Delegierte Berechtigungen hinzufügen:

a. In Ihrer App navigieren API Berechtigungen

B. Klicken Sie auf Eine Erlaubnis hinzufügen um die erforderlichen Berechtigungen hinzuzufügen, die die App sollte haben. Zum Beispiel, um den Lese-/Lesezugriff auf SharePoint zu ermöglichen Microsoft Abbildung → Delegierte Berechtigungen → Standorte → Sites. ReadWrite. Alle . Die erforderliche Berechtigungen hängen davon ab, wie Sie die App in KNIME Workflows verwenden möchten (für eine Liste der gemeinsamen Anwendungsbereiche Abschnitt

<a href="#page25" style="color: #ff6600; text-decoration: un

c. Klicken Sie auf Berechtigungen hinzufügen



d. Wenn angezeigt, klicken Sie auf Grant admin Zustimmung für ... Admin-Einwilligung für alle hinzugefügten API Berechtigungen. In diesem Fall werden die Nutzer während der Einwilligung nicht aufgefordert interaktive Authentifizierung mehr.

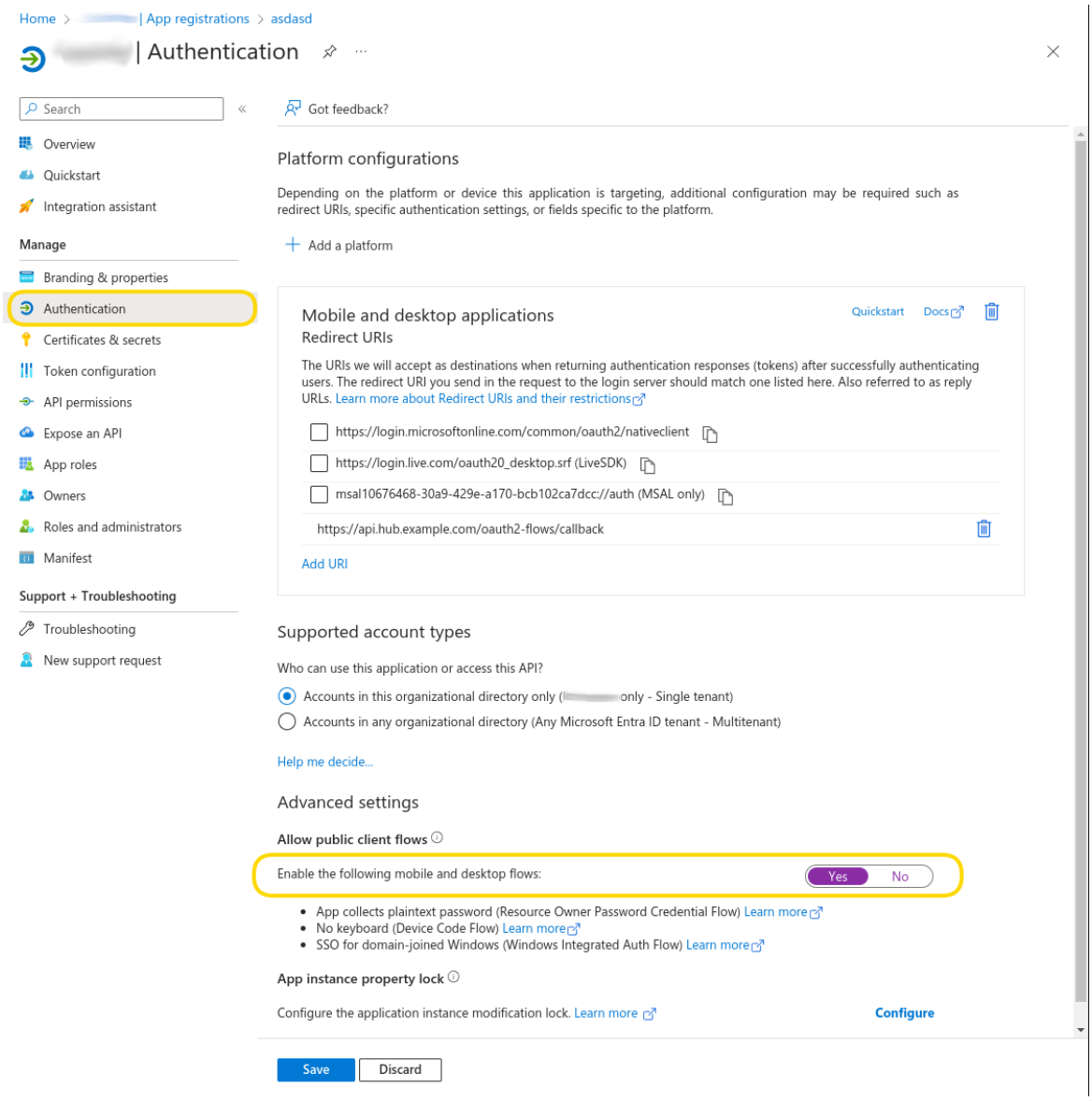
5. Nur wenn Sie die App mit Geheimnissen des Typs verwenden müssen (gefördert):

<a href="#page23" style="color: #ff6600; text-

a. In Ihrer App navigieren Authentifizierung → Öffentliche Kundenströme

B. Setzen Sie den Schieber Ja.

c. Klicken Sie auf Speichern



d. Navigieren API Berechtigungen , fügen Sie alle erforderlichen API-Berechtigungen und Zustimmung zu wie in Schritt 6 oben.

6. Retrieve the Application ID:

a. In Ihrer App navigieren Überblick

B. Kopieren Sie dieAnmeldung (Client) ID

7. In Ihrem KNIME Hub Geheimnis(n):

a. Den Antragsausweis in die Client/App ID Feld

API-Berechtigungen, auch Scopes genannt, handeln als Obergrenze für das, was getan werden kann mit dem erworbenen Zugriffstoken. Darüber hinaus, die meisten Dienstleistungen in der Microsoft/Azure Plattform auferlegen **zusätzlich** Berechtigungsprüfungen basierend auf der Rollen und Gruppen des Benutzers. Beispiele sind SharePoint Berechtigungen oder Azure RBAC .

Bereiten Sie eine Azure-App für Anwendungs- oder Serviceprinzipien vor

So wird beschrieben, wie man eine Azure App einrichten kann, so dass sie mit Geheimnissen des Typs verwendet werden kann
<a href="#page23" style="color: #ff6600; text-decoration: underline;">Microsoft · Anwendungs-/Dienstle
.

Voraussetzungen:

- Zulassung zur Registrierung von Apps in Azure Entra ID. Azure Admins haben in der Regel diese die Genehmigung, kann aber auch durch Rollen wie die Anwendung Administrator oder Anwendung Entwickler (siehe Hier.)

Schritte:

ANHANG Einloggen in die Azure Portal

2. Navigieren zu Azure Entra ID → Anmeldungen der App

3. Eine neue App registrieren:

   a. Klicken Sie auf Neue Anmeldung

   B. Geben Sie einen Namen ein und wählen Sie den unterstützten Kontotyp (Einzelmiete in den meisten Rechtssachen Eine Umleitung URI ist nicht erforderlich.

   c. Klicken Sie auf Register

L 347 vom 20.12.2013, S. 1). Anwendungsberechtigungen hinzufügen:

   a. In Ihrer App navigieren API Berechtigungen

   B. Klicken Sie auf Eine Erlaubnis hinzufügen um die erforderlichen Berechtigungen hinzuzufügen, die die App sollte haben. Zum Beispiel, um den Lese-/Lesezugriff auf SharePoint zu ermöglichen Microsoft Abbildung → Bewerbungsrechte → Standorte → Sites. ReadWrite. Alle . Die erforderliche Berechtigungen hängen davon ab, wie Sie die App in KNIME Workflows verwenden möchten (für eine Liste der gemeinsamen Anwendungsbereiche <a href="#page25" style="color: #ff6600; text-decoration: un Abschnitt

   c. Klicken Sie auf Berechtigungen hinzufügen

   d. Klicken Sie auf Grant admin Zustimmung für ... Admin-Einwilligung für alle hinzugefügten API Berechtigungen.

5. Erstellen Sie ein Anwendungsgeheimnis:

   a. In Ihrer App navigieren Zertifikate & Geheimnisse → Client-Geheimnisse

   B. Klicken Sie auf Neues Client Geheimnis_

   c. Beschreibung und Ablauf

   d. Klicken Sie auf Hinzufügen

   e. Kopieren Sie die Wert des neu erstellten Client-Geheimnisses, wie es nur einmal nach die Schöpfung.

6. Retrieve the Application ID:
   a. In Ihrer App navigieren Überblick
   B. Kopieren Sie dieAnmeldung (Client) ID
7. In Ihrem KNIME Hub Geheimnis(n):
   a. Den Antragsausweis in die Client/App ID Feld
   B. Das Client-Geheimnis in die Client/App Secret Feld

> API-Berechtigungen, auch Scopes genannt, handeln als Obergrenze für das, was getan werden kann mit dem erworbenen Zugriffstoken. Darüber hinaus, einige Dienstleistungen in der Microsoft/Azure Plattform auferlegen **zusätzlich** Berechtigungsprüfungen basierend auf Rollen und Gruppenmitgliedschaften des Diensteleiters. Ein Beispiel dafür ist Azure RBAC .

Erstellen einer Azure Storage SAS URL

So wird beschrieben, wie man eine Azure Storage SAS URL erstellt, so dass sie mit
<a href="#page24" style="color:#000000; text-decoration: underline;">Geheimnisse des Typs Azure Storage fre
. Eine SAS URL gewährt eingeschränkt und zeitbegrenzter Zugriff auf einen Azure-Speicherbehälter oder Objekte innerhalb eines Behälters.

Voraussetzungen:

- Erlaubnis, SAS-URLs zu erstellen, je nach Art der SAS zu erstellen. Vgl. Hier. für eine Überblick.

Um eine Azure Storage SAS URL für einen Container zu erstellen

ANHANG Einloggen in dieAzure Portal

2. Navigieren zu Speicherkonten → Ihr Konto → Container → Ihr Container → Geteilte Zugriffstoken
3. Geben Sie die Anmeldemethode, die Berechtigungen und die Ablaufinformationen ein
4. Klicken Sie aufSAS-Token und URL generieren
5. Kopieren Sie dieBlob SAS URL
6. In Ihrem KNIME Hub Geheimnis(n): Die Polizei einfügen Blob SAS URL in der SAS URL Feld

Die Schritte zum Erstellen von SAS URL für ein bestimmtes Objekt innerhalb eines Containers sind ähnlich. Navigieren das Objekt, klicken Sie darauf und wählen Sie dann SAS generieren .

Finden Sie Ihren Azure Storage gemeinsamen Schlüssel

So beschreibt man, wie man den gemeinsamen Schlüssel eines Azure-Speicherkontos lokalisiert, so dass es
Hier.
. Ein solcher Schlüssel gewährt uneingeschränkt

Zugriff auf ein Azure Storage-Konto und alle Container innerhalb.

Voraussetzungen:

- Erlaubnis, die Kontoschlüssel des Speicherkontos anzuzeigen. Mehrere Rollen wie beschrieben

  Hier. ermöglichen, Kontoschlüssel anzuzeigen.

Der gemeinsame Schlüssel für einen Azure Storage Container finden Sie wie folgt:

ANHANG Einloggen in die Azure Portal

2. Navigieren zu Speicherkonten → Ihr Konto → Zugriffsschlüssel

3. Kopieren eines der gezeigten Tasten

L 347 vom 20.12.2013, S. 1). In Ihrem KNIME Hub Geheimnis(n): Den kopierten Schlüssel in das Schlüssel Feld

Architektur

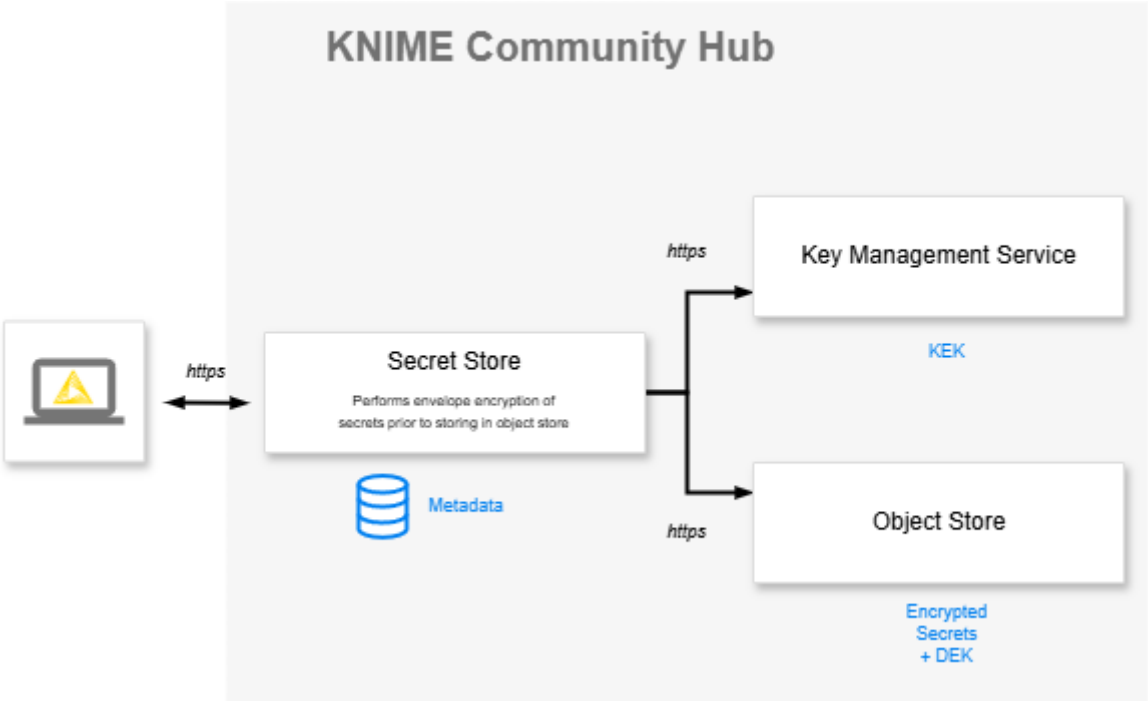


Abbildung 1. KNIME Secrets Store Architektur auf dem KNIME Community Hub. Der geheime Store besteht aus drei Komponenten: dem Secret Store Service, dem Key Management Service, der speichert den Schlüsselverschlüsselungsschlüssel (KEK) und den Object Store, der verschlüsselte Geheimnisse speichert und ihre Datenverschlüsselungsschlüssel(DEK). Alle Kommunikation ist über TLS gesichert.

Der KNIME Secret Store besteht aus drei Hauptdienstleistungen:

- Secret Store Service
- Schlüsselverwaltung Service
- Einloggen

Alle Kommunikation ist über **TLS-Verschlüsselung** .

- **Secret Store Service** : ist die Kernkomponente, die für die Verwaltung von Geheimnissen in der KNIME Community Hub.
  Der Secret Store Service speichert nicht-sensitive Metadaten, die mit jedem Geheimnis zusammenhängen, wie Name und Beschreibung des Geheimnisses, in einer relationalen Datenbank.
  Der Secret Store Service verschlüsselt sensible Daten mit Hüllkurvenverschlüsselung.
- **Key Management Service** : Envelope-Verschlüsselung wird mit der AWS Verschlüsselung SDK und der Key Management Service.
- **Einloggen** : Sobald das Geheimnis verschlüsselt ist, wird es im Object Store mit Server gespeichert. Seitenverschlüsselung.

Envelope Verschlüsselung ist ein hybrides kryptographisches System von großen Cloud-Anbietern wie

Amazon, Microsoft und Google.

Es verwendet zwei Arten von Schlüsseln:

ANHANG Ein einzigartiger Datenverschlüsselungsschlüssel (DEK) für jedes Geheimnis

2. Ein Schlüsselverschlüsselungsschlüssel (KEK), der periodisch für eine verbesserte Sicherheit gedreht wird.

Prüfung

Der Secret Store bietet Auditing-Funktionalität, um Nutzeraktivitäten zu verfolgen und zu analysieren. Prüfung logs sind nützlich, um potenzielle Sicherheitsprobleme zu identifizieren und die Einhaltung von Organisationspolitik.

Auditprotokolle sind **60 Tage erhalten** und tun **keine sensiblen Informationen enthalten** , wie Passwörter oder Zugriffstoken.

Protokollinhalt des Audits

Jeder Audit-Log-Eintrag enthält strukturierte Informationen über eine Aktion, die in der Geheimspeicher:

- **Art der Maßnahme**

  Beschreibt, was mit dem Artikel passiert ist, zum Beispiel, hinzugefügt, aktualisiert, verbraucht oder entfernt.

- **Ereigniskennzeichen**

  Korrelations-ID – Gruppen verwandten Ereignisse in einem einzigen Fluss.

  Event-ID – Einzigartige Kennung des einzelnen Ereignisses.

- **Veranstaltungsinitiator**

  Erkennt, wer das Ereignis ausgelöst hat, einschließlich ihrer **Benutzername**und **Kennung** .

- **Artikeldetails**

  Bietet Informationen über den betroffenen Artikel, einschließlich:

  - Einzigartige Artikel-ID
  - Artikeltyp (z.B. geheim, Workflow)
  - Betreffinformationen wie Name, Schema oder Konfiguration

- **Allgemeine Informationen**

  Definiert den organisatorischen Kontext, in dem sich der Gegenstand befindet, wie die **Team oder Name des Arbeitsraums** und **Umfang Konto ID** .

- **Formatversion**

  Interne Versionsnummer des Audit-Log-Formats.

- **Zeitstempel**

  Aufzeichnungen, wenn das Ereignis aufgetreten ist.

- **Stellenangebote** **(nur enthalten, wenn das Ereignis von einem Job auf dem lokalen Hub stammt)**

  Enthält Metadaten über den ausgeführten Job, einschließlich:

- Job-ID und Name
- Kontext und Ausführung
- Einsatzart
- Workflow Referenz (Hub ID, Pfad, Version)
- Job-Initiator-Details (Name und Konto-ID)

Prüfprotokolleinträge

Das folgende JSON-Beispiel zeigt Audit-Log-Einträge für das Erstellen, Bearbeiten, Konsumieren und ein Geheimnis löschen:


```
(
{\cHFFFF}
"Aktion": "gefüttert",
"korrelationId": "c5bd2e2e-c831-437a-be41-ef1719b923:01",
"eventId": "1aeeebf0-9dd5-4eca-be43-db996db55c1b",
"eventInitiator": "knimeadmin",
"eventInitiatorAccountId": "Konto:Benutzer:618a54bf-894a-45c4-84a4-2105e78c68dc",
"formatVersion": 1,
"itemId": "secret:bd071853-bfcc-47de-8779-e22ed2cf99df",
"itemType": "geheim",
"scope": "Initial Team",
"scopeAccountId": "Konto:team:02a80269-dc98-47f6-8b57-024df090a472",
"subject": {\cHFFFF}
"config": {\cHFFFF}
"username": "sdasad"
},
"configSchema": "credentials",
"Name": "mysecret"
},
"Zeitstempel": "2025-09-04T13:26:07.708Z"
},
{\cHFFFF}
"Aktion": "updated",
"KorrelationId": "ef07e583-a507-4eaf-b15c-e4bd6c254df6:01",
"eventId": "8e48231c-5654-495c-b739-eb50cf9d09f4",
"eventInitiator": "knimeadmin",
"eventInitiatorAccountId": "Konto:Benutzer:618a54bf-894a-45c4-84a4-2105e78c68dc",
"formatVersion": 1,
"itemId": "secret:bd071853-bfcc-47de-8779-e22ed2cf99df",
"itemType": "geheim",
"scope": "Initial Team",
"scopeAccountId": "Konto:team:02a80269-dc98-47f6-8b57-024df090a472",
"subject": {\cHFFFF}
"config": {\cHFFFF}
"username": "sdasad"
```

},
"configSchema": "credentials",
"Name": "mysecret"
},
"Zeitstempel": "2025-09-04T13:27:11.401Z"
},
{\cHFFFF}
"Aktion": "Verbraucht",
"KorrelationId": "99c3a5d7-936e-4f2b-a349-7f3606860a58:01",
"eventId": "831dc182-7ba0-4602-a40a-87244b38930a",
"eventInitiator": "knimeadmin",
"eventInitiatorAccountId": "Konto:Benutzer:618a54bf-894a-45c4-84a4-2105e78c68dc",
"formatVersion": 1,
"itemId": "secret:bd071853-bfcc-47de-8779-e22ed2cf99df",
"itemType": "geheim",
"scope": "Initial Team",
"scopeAccountId": "Konto:team:02a80269-dc98-47f6-8b57-024df090a472",
"subject": {\cHFFFF}
"config": {\cHFFFF}
"username": "sdasad"
},
"configSchema": "credentials",
"Name": "mysecret"
},
"Zeitstempel": "2025-09-04T13:43:09.0293050152"
},
{\cHFFFF}
"Aktion": "Verbraucht",
"korrelationId": "e5087688-9f18-4643-8ef3-45de6064a2e2:02",
"eventId": "ea3a6d56-dcbb-4ae4-8e58-224c12414a32",
"eventInitiator": "knimeadmin",
"eventInitiatorAccountId": "Konto:Benutzer:618a54bf-894a-45c4-84a4-2105e78c68dc",
"formatVersion": 1,
"itemId": "secret:bd071853-bfcc-47de-8779-e22ed2cf99df",
"itemType": "geheim",
"job":
"executionContextId": "2319a554-81d7-47a9-82a9-846cbb0fcbd8",
"id": "80a42d53-bd32-4ca1-beb6-4e849df248da",
"Initiator": "knimeadmin",
"InitiatorAccountId": "Ergebnis:618a54bf-894a-45c4-84a4-2105e78c68dc",
"Name": "SecretConsumeTest 2025-09-04 13.43.38",
"scope": "account:team:02a80269-dc98-47f6-8b57-024df090a472",
"Workflow": "/Benutzer/Initial Team/Initial Space/SecretConsumeTest",
"WorkflowId": "*d3Xjp31o9gbSjBw"
},
"scope": "Initial Team",
"scopeAccountId": "Konto:team:02a80269-dc98-47f6-8b57-024df090a472",
"subject": {\cHFFFF}
"config": {\cHFFFF}
"username": "sdasad"
},
"configSchema": "credentials",

"Name": "mysecret"
},
"Zeitstempel": "2025-09-04T13:43:51.778383302Z"
},
{\cHFFFF}
"Aktion": "entfernt",
"KorrelationId": "a1c1c21a-24b7-494b-a57b-8680d747eb50:01",
"eventId": "e448132e-3956-49bd-b813-a39abe1b9893",
"eventInitiator": "knimeadmin",
"eventInitiatorAccountId": "Konto:Benutzer:618a54bf-894a-45c4-84a4-2105e78c68dc",
"formatVersion": 1,
"itemId": "secret:bd071853-bfcc-47de-8779-e22ed2cf99df",
"itemType": "geheim",
"scope": "Initial Team",
"scopeAccountId": "Konto:team:02a80269-dc98-47f6-8b57-024df090a472",
"subject": {\cHFFFF}
"configSchema": "credentials",
"Name": "mysecret"
},
"Zeitstempel": "2025-09-04T13:46:34.090026679Z"
}
!

KNIME AG
Talacker 50
8001 Zürich, Schweiz
www.knime.com
Info@knime.com