

HULFT Squareアプリケーション仕様書

Snowflake-EntraID_プロビジョニング

1.0 版 | 2024 年 10 月 8 日

Snowflake-EntraID_プロビジョニング HULFT Squareアプリケーション Overview

本アプリケーションについて

本アプリケーションは、Snowflakeをデータ分析基盤として全社員で利用する際、Microsoft Entra IDと連携することでプロビジョニングを行うためのスクリプトサンプルをアプリケーション化したものです。
具体的には以下の処理が含まれます。

- ・ Microsoft Entra IDからパブリック IP を取得し、Snowflake上のネットワークルールのパブリック IPを洗い替える。
- ・ Microsoft Entra IDとのSCIM連携によって作成されたSnowflake上のユーザーにロールを付与し、デフォルトロール・ウェアハウスを対象ユーザ分複数回繰り返し設定する。
- ・ Microsoft Entra IDとのSCIM連携によって無効化されたSnowflake上のユーザを対象件数分削除する。

スクリプトをコピー後、状況に合わせてワークスペース・コネクション等カスタマイズすることを推奨します

INDEX

スクリプト利用手順

- ・ コネクション設定(Azure側)
- ・ ワークスペース設定とフォルダ作成(HULFT Square側)
- ・ コネクション設定(HULFT Square側)
- ・ スクリプト利用上注意

スクリプト詳細

- ・ スクリプト設定 (Azure_get_Service_IPs)
- ・ スクリプト設定 (Snowflake_alter_network_rule)
- ・ スクリプト設定(Snowflake_grant_role)
- ・ スクリプト設定(Snowflake_delete_user)

Snowflake-EntraID_プロビジョニング HULFT Squareアプリケーション ワークスペース設定とフォルダ作成(HULFT Square側)

ワークスペース設定とフォルダ作成

HULFT Square アプリケーションの動作に必要なワークスペース設定とAPIから取得したデータを格納するフォルダを作成します

ワークスペース設定

コネクションとプロジェクトとAPIから取得したデータを格納するワークスペースを作成します

※すでにワークスペースが利用可能な場合、本手順は不要です

ワークスペース設定(オレンジ色項目は必須項目)

名前	環境に合わせて任意選択
説明	任意
ユーザー	環境に合わせて任意選択
グループ	環境に合わせて任意選択

フォルダ作成

APIから取得したデータを格納するフォルダを作成します

※任意のワークスペースを作成した上で、以下のフォルダを作成します

ストレージ設定(オレンジ色項目は必須項目)

ワークスペース	環境に合わせて任意選択
ディレクトリ名	Azure_Public_IP_取得

Snowflake-EntraID_プロビジョニング HULFT Squareアプリケーション コネクション設定(Azure側)

コネクション設定

HULFT SquareからAzure REST APIへの接続に必要な設定に関して記述します

Azure側設定(前提条件)

- 以下Azureサービスの「アプリの登録」においてアプリ登録を行い、APIの利用が可能であることを確認します
<https://learn.microsoft.com/ja-jp/entra/identity-platform/quickstart-register-app?tabs=certificate>
- 登録したアプリケーション内でクライアントシークレットを作成してください。
- 登録したアプリケーションから以下の値をメモしておきます。

tenant_id
client_id
client_secret

ホーム > [検索] ✕ ...

検索 [] ◊ << 削除 [] エンドポイント [] プレビュー機能 []

概要

クイック スタート
統合アシスタント
問題の診断と解決
管理
ブランド化とプロパティ
認証
証明書とシークレット

少しお時間があれば、Microsoft ID プラットフォーム (以前は開発者向け Azure AD) に関するフィードバックをぜひお寄せください。 →

基本

表示名	:	[]	クライアントの資格情報	:	0 証明書、1 シークレット
アプリケーション (クライアント) ID	:	[]	リダイレクト URI	:	0 個の Web、1 個の SPA、0 個のバックグラウンド クライアント
オブジェクト ID	:	[]	アプリケーション ID の URI	:	api: []
ディレクトリ (テナント) ID	:	[]	ローカル ディレクトリでのマネ...	:	[]
サポートされているアカウント...	:	所属する組織のみ			

ホーム > DSS_REST_API

[] | 証明書とシークレット ✕ ...

検索 [] ◊ << フィードバックがある場合 []

概要

クイック スタート
統合アシスタント
問題の診断と解決
管理
ブランド化とプロパティ
認証
証明書とシークレット

資格情報は、Web アドレスの指定が可能な場所 (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うことをお勧めします。

アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。

証明書 (0) クライアント シークレット (1) フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアント シークレット

説明	有効期限	値	シークレット ID
[]	2026/4/22	Jo8*****	[]

Azure API仕様

- 本スクリプトでは以下のService Tags - List APIを使用しております。APIの詳細仕様は以下公式ドキュメントよりご確認ください。
<https://learn.microsoft.com/ja-jp/rest/api/virtualnetwork/service-tags/list?view=rest-virtualnetwork-2024-01-01&tabs=HTTP>

Snowflake-EntraID_プロビジョニング HULFT Squareアプリケーション コネクション設定(HULFT Square側)

コネクション設定

HULFT SquareとAzure REST APIの接続に必要な設定に関して記述します

HULFT Square側設定

APIリクエストを送信するための設定を作成します

アクセストークン取得用コネクション設定(オレンジ色項目は必須項目)

コネクタータイプ	REST接続
名前	REST接続設定_Azure_REST_login
ワークスペース	環境に合わせて任意選択
説明	任意
URL設定	https://login.microsoftonline.com
プロファイル	任意
備考	認証用のコネクション。アクセストークンを取得する際に使用する。

リクエスト用コネクション設定(オレンジ色項目は必須項目)

コネクタータイプ	REST接続
名前	REST接続設定_Azure_REST_management
ワークスペース	環境に合わせて任意選択
説明	任意
URL設定	https://management.azure.com
プロファイル	任意
備考	パブリック IP取得用のコネクション。Service Tagごとのパブリック IPを取得する際に使用する。

コネクション設定

HULFT SquareとSnowflakeの接続に必要な設定は以下の通り

HULFT Square側設定

Snowflakeに接続するための設定を作成する

- ・既にSnowflake接続設定が存在する場合、既存のコネクションを使用することも可。
- ・ネットワークルールと紐づいているデータベース名・スキーマ名を選択されているコネクション設定が必要。

接続用コネクション設定

コネクタータイプ	Snowflake接続設定
アカウント識別子	https://xxxx.xxxxxxxx.snowflakecomputing.com
ウェアハウス名	任意のウェアハウス名
データベース名	SNOWFLAKE
スキーマ名	ACCOUNT_USAGE
Enter URL directly	必要に応じてチェックする
URLを直接入力する	必要に応じて「Enter URL directly」にチェックを入れパラメータ「role=<適切な権限を持つロール名>」を追加する
ユーザ名	任意のユーザ名
パスワード	上記ユーザのパスワード

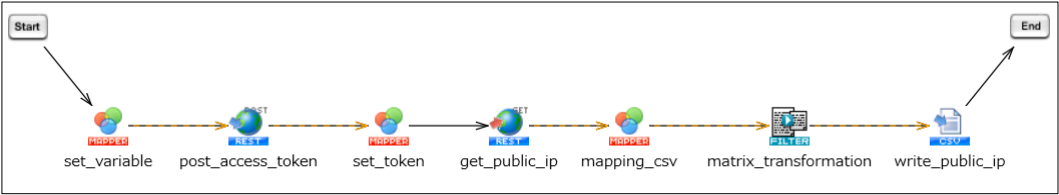
Snowflake-EntralID_プロビジョニング HULFT Squareアプリケーション スクリプト利用上注意

利用について

- ・本スクリプトは外部のデータ提供元に接続しデータを取得します
- ・本スクリプトの利用者はデータ提供元の利用規約に同意した上でスクリプトを利用してください
- ・取得されるデータの正確性、完全性、最新性、網羅性等のデータに対する内容はスクリプト上では保証されません
- ・データ提供元のサービス提供の変更やAPI仕様変更に対して、本スクリプトでは保証されません

Snowflake-EntraID_プロビジョニング HULFT Squareアプリケーション
スクリプト設定(Azure_get_Service_IPs)

スクリプト全体図



* 各設定のオレンジ色の設定箇所は、アプリケーションをインストールするだけでは設定されないため、アプリケーションをインストール後に手動で入力してください

スクリプト動作概要

Azure REST API を使用して、提供するサービスごとのパブリック IP を取得し CSV ファイルへ出力します。
取得した CSV は以下に格納されます

CSV格納先	/[指定したワークスペース名]/Azure_Public_IP_取得/Azure_Service_Tags_List.csv
--------	--

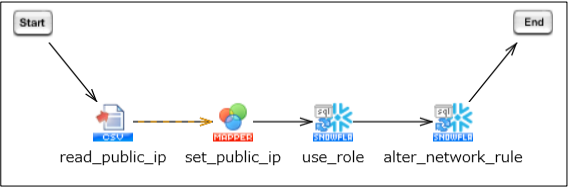
スクリプト変数

I_tenant_id	Azureに登録したアプリケーションより取得した値を入力
I_location	取得したいロケーションの名称を入力
I_subscriptionId	アプリケーションに登録したサブスクリプションIDを入力
I_systemService	AzureAD ※この記述を変更することで、他のAzureサービスのパブリック IP を取得することも可能です。
I_AccessToken	スクリプト内で取得するため初期値無し
I_client_secret	Azureに登録したアプリケーションで作成したクライアントシークレットの値を入力
I_client_id	Azureに登録したアプリケーションより取得した値を入力
LC_resource	https://management.core.windows.net/
LC_grant_type	client_credentials
LC_api-version	2024-01-01

※API仕様についてはデータ提供元のAPI仕様書を参照ください
<https://learn.microsoft.com/ja-jp/rest/api/virtualnetwork/service-tags/list?view=rest-virtualnetwork-2024-01-01&tabs=HTTP>

Snowflake-EntraID_プロビジョニング HULFT Squareアプリケーション
スクリプト設定(Snowflake_alter_network_rule)

スクリプト全体図



* 各設定のオレンジ色の設定箇所は、アプリケーションをインストールするだけでは設定されないため、アプリケーションをインストール後に手動で入力してください

スクリプト動作概要

Azure のパブリック IP が書き込まれた CSV ファイルを読み取り、Snowflake の指定したネットワークルールに登録された IP を洗い替えます。
読み取る CSV ファイルは以下に格納します。

CSV格納先	/[指定したワークスペース名]/Azure_Public_IP_取得/Azure_Service_Tags_List.csv
--------	--

スクリプト変数

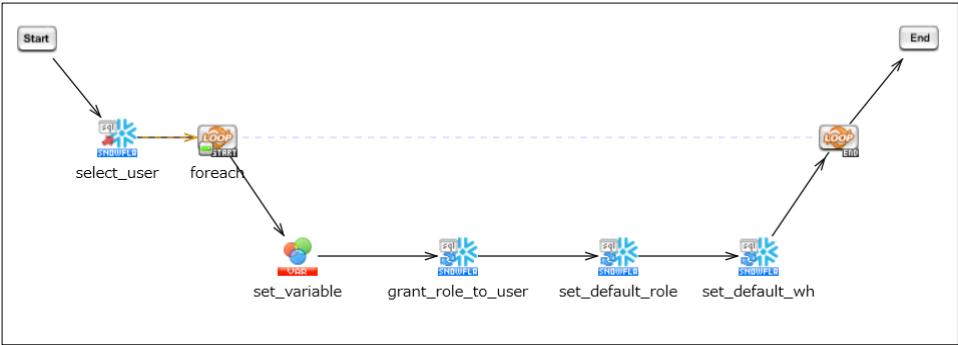
L_Public_IP	CSVファイルから読み込んだIPを格納します。
L_NETWORK_RULE_NAME	IPを洗い替えたいネットワークルールの名前を入力

コンポーネント名	
use_role	
 use_role	
コンポーネント概要	
ネットワークルールをALTER NETWORK RULEできる権限を設定する。 ※必須設定以外はそのまま問題無し。	
必須設定	
接続先	対象ネットワークルールと紐づいているデータベース名・スキーマ名を選択されているコネクションを選択する。
SQL文	USE ROLE ACCOUNTADMIN; ※対象ネットワークルールを操作できるロールをUSE ROLEする。

コンポーネント名	
alter_network_rule	
 alter_network_rule	
コンポーネント概要	
対象ネットワークルールにIPの洗い替えを行う。 ※必須設定以外はそのまま問題無し。	
必須設定	
接続先	対象ネットワークルールと紐づいているデータベース名・スキーマ名を選択されているコネクションを選択する。
SQL文	ALTER NETWORK RULE "\${NETWORK_RULE_NAME}" SET VALUE_LIST = (\${Public IP});

Snowflake-EntraID_プロビジョニング HULFT Squareアプリケーション
スクリプト設定(Snowflake_grant_role)

スクリプト全体図



* 各設定のオレンジ色の設定箇所は、アプリケーションをインストールするだけでは設定されないため、アプリケーションをインストール後に手動で入力してください

スクリプト動作概要

スクリプト変数

I_ROLE	ユーザに付与したロールを入力。※このロールをデフォルトウェアロールにも設定する。
I_LOGIN_NAME	Snowflakeに新たにプロビジョニングされたユーザが格納される。
I_WAREHOUSE	デフォルトウェアハウスに設定したいウェアハウスを入力。

コンポーネント名	
select_user	 select_user
コンポーネント概要	
Snowflake上にプロビジョニングされたユーザを抽出する。	
必須設定	
接続先	"SNOWFLAKE"."ACCOUNT_USAGE"."USERS"にアクセスできる権限を持ったコネクションを選択する。
SQL文	<pre>SELECT "NAME" ,"CREATED_ON" ,"DELETED_ON" ,"LOGIN_NAME" ,"DISPLAY_NAME" ,"FIRST_NAME" ,"LAST_NAME" ,"EMAIL" ,"MUST_CHANGE_PASSWORD" ,"HAS_PASSWORD" ,"COMMENT" ,"DISABLED" ,"SNOWFLAKE_LOCK" ,"DEFAULT_WAREHOUSE" ,"DEFAULT_NAMESPACE" ,"DEFAULT_ROLE" ,"EXT_AUTHN_DUO" ,"EXT_AUTHN_UID" ,"BYPASS_MFA_UNTIL" ,"LAST_SUCCESS_LOGIN" ,"EXPIRES_AT" ,"LOCKED_UNTIL_TIME" ,"HAS_RSA_PUBLIC_KEY" ,"PASSWORD_LAST_SET_TIME" FROM "SNOWFLAKE"."ACCOUNT_USAGE"."USERS" WHERE "DEFAULT_ROLE" IS NULL AND "DELETED_ON" IS NULL AND "EMAIL" IS NOT NULL AND "DISABLED" = 'false' ;</pre>

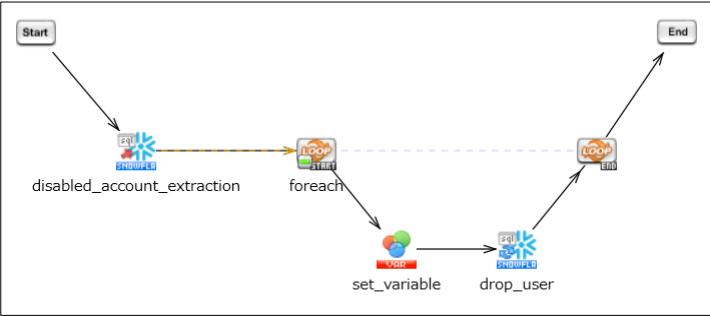
コンポート名	
grant_role_to_user	
	
grant_role_to_user	
コンポーネント概要	
対象ユーザにロールを付与する。	
必須設定	
接続先	対象ユーザにロールを付与できるコネクションを選択する。
SQL文	GRANT ROLE "\${L_ROLE}" TO USER "\${L_LOGIN_NAME}";

コンポート名	
set_default_role	
	
set_default_role	
コンポーネント概要	
対象ユーザにデフォルトロールを設定する。	
必須設定	
接続先	対象ユーザにデフォルトロールを付与できるコネクションを選択する。
SQL文	ALTER USER "\${L_LOGIN_NAME}" SET DEFAULT_ROLE = "\${L_ROLE}";

コンポート名	
set_default_wh	
	
set_default_wh	
コンポーネント概要	
対象ユーザにデフォルトウェアハウスを設定する。	
必須設定	
接続先	対象ユーザにデフォルトウェアハウスを付与できるコネクションを選択する。
SQL文	ALTER USER "\${L_LOGIN_NAME}" SET DEFAULT_WAREHOUSE = "\${L_WAREHOUSE}";

Snowflake-EntraID_プロビジョニング HULFT Squareアプリケーション
スクリプト設定(Snowflake_delete_user)

スクリプト全体図



* 各設定のオレンジ色の設定箇所は、アプリケーションをインストールするだけでは設定されないため、アプリケーションをインストール後に手動で入力してください

スクリプト動作概要

スクリプト変数

L_LOGIN_NAME	Snowflake上で無効化されたユーザが格納されます。
--------------	------------------------------

コンポート名	
disabled_account_extraction	
	
disabled_account_extraction	
コンポーネント概要	
Snowflake上で無効化されたユーザを抽出する。	
必須設定	
接続先	"SNOWFLAKE"."ACCOUNT_USAGE"."USERS"にアクセスできる権限を持ったコネクションを選択する。
SQL文	<pre>SELECT A."LOGIN_NAME" FROM "SNOWFLAKE"."ACCOUNT_USAGE"."USERS" A INNER JOIN (SELECT "LOGIN_NAME" ,MAX("CREATED_ON") "CREATED_ON" FROM "SNOWFLAKE"."ACCOUNT_USAGE"."USERS" GROUP BY "LOGIN_NAME") B ON A."LOGIN_NAME" = B."LOGIN_NAME" AND A."CREATED_ON" = B."CREATED_ON" WHERE A."DISABLED" = 'true' AND A."DELETED_ON" IS NULL ;</pre>

コンポート名	
drop_user	
	
drop_user	
コンポーネント概要	
対象ユーザのDROPを行う	
必須設定	
接続先	ユーザをDROPできる権限を持ったコネクションを選択する。
SQL文	DROP USER IF EXISTS "\${L_LOGIN_NAME}";