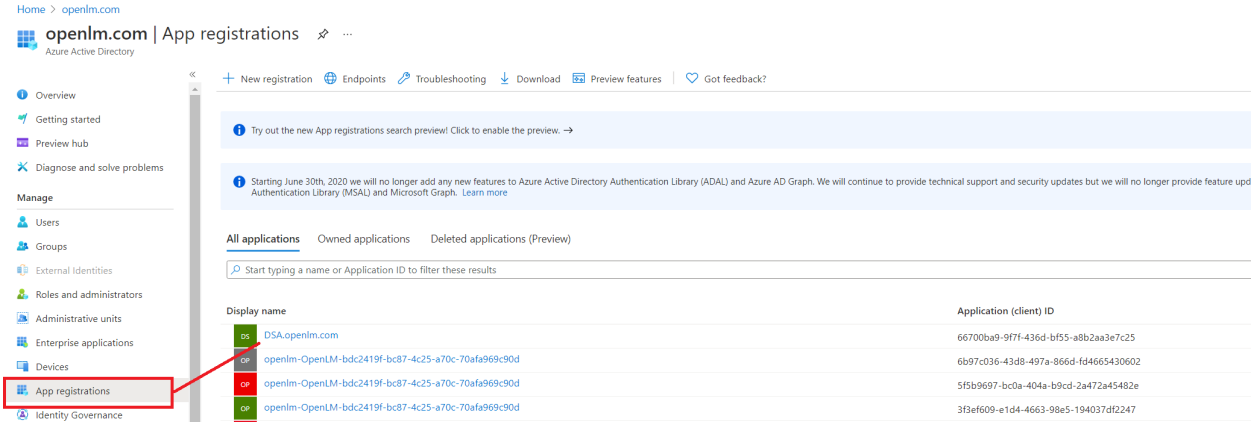
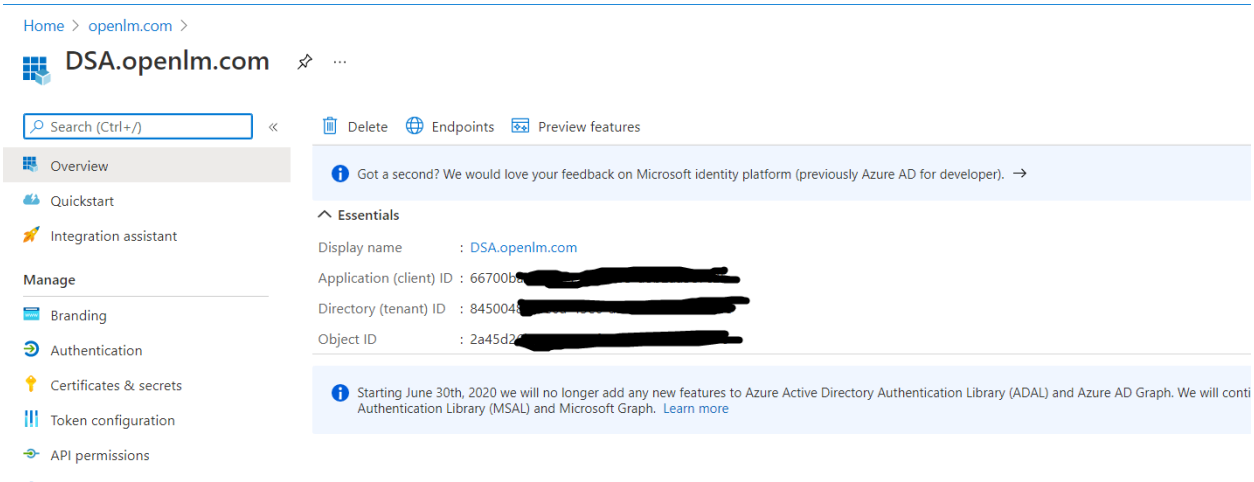
Microsoft Graph テクノロジを使用して Azure AD からデータを取得する場合、自分または Azure ポータルで構成を行う必要があります。

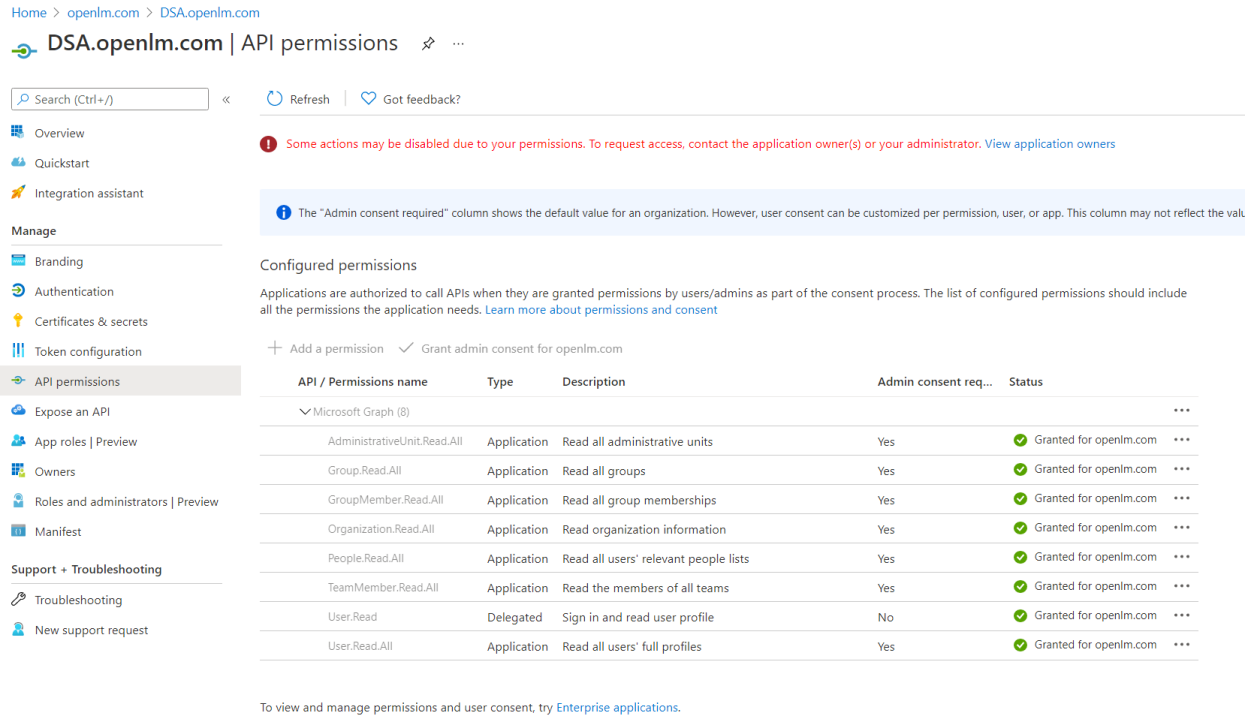
1. ディレクトリへのアクセスを許可するために使用されるアプリケーションを登録します。



2. 登録時に、パラメータ client_id、tenant_id、client_secret を取得します。最後は 1 回だけ表示されるため、ユーザーは覚えておく必要があります。これらのパラメーターは、Azure AD の DSS UI ドメイン設定で入力する必要があります (client_secretは DSS DB で暗号化されます)。これらのパラメーターは、Microsoft Graph サービスに接続して承認するために DSA によって使用され、Azure ディレクトリに関するデータが返されます。



3. アプリケーションにアクセス許可を付与します (DSA がデータを取得できるようにするため)。



ディレクトリ同期 Azure ディレクトリ

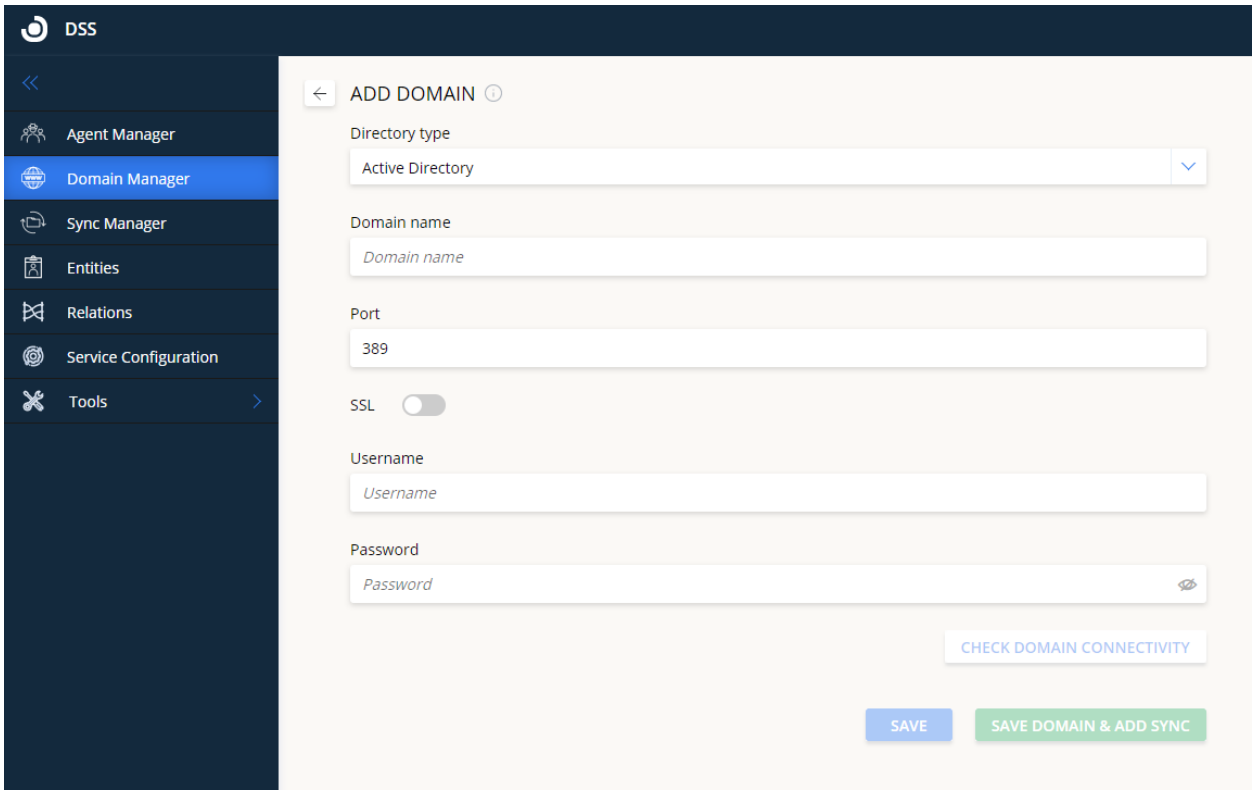
ドメインの追加

新しいディレクトリ タイプ Azure Directory をドメイン マネージャー画面に追加します

選択しそれに応じて以下のフィールドを更新します

1. ドメイン名 : フリーテキスト
2. ディレクトリ (tenant) ID -**NEW**
3. アプリケーション (client) ID -**NEW**
4. クライアントシークレット -**NEW**

アプリケーション (client) ID とクライアント シークレットは、Azure ディレクトリ (tenant) ID による認証に使用されます。



ドメイン接続のチェックと保存ボタンはそのままにしておきます...

同期設定

目的地と時刻

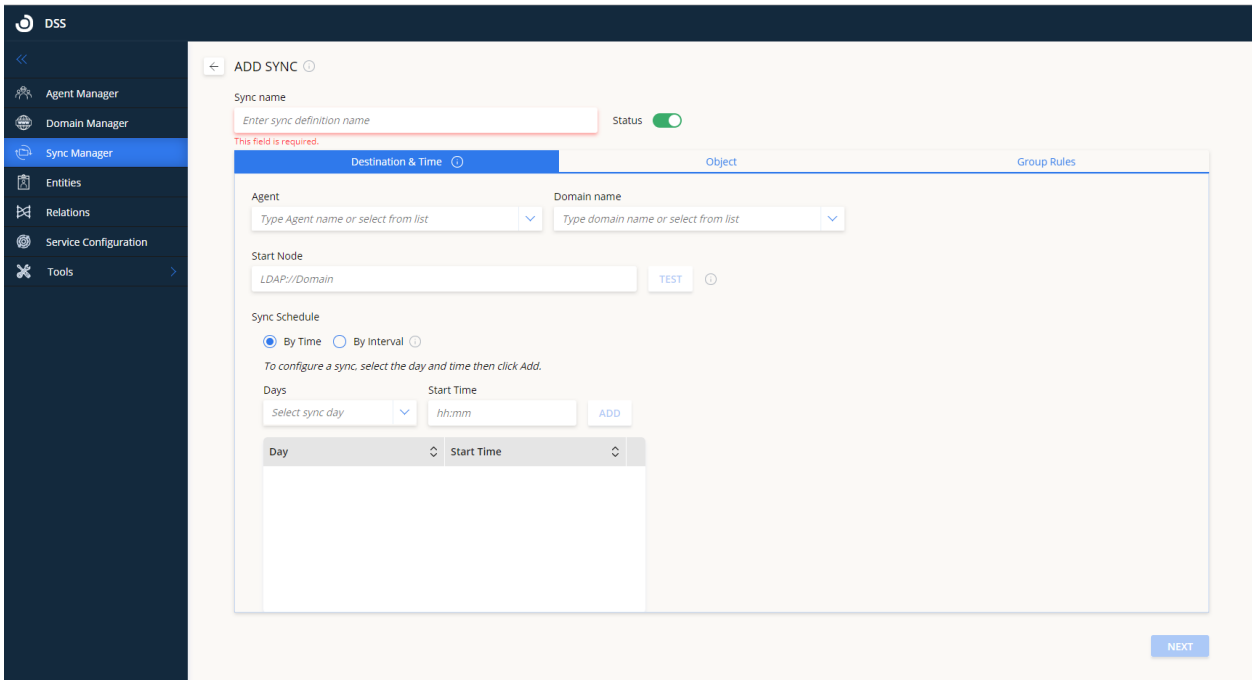
開始ノードのオプション: LDAP ディレクトリとは異なり、Azure の構造は異なります: ユーザーは次のことを行うことができます。

1. 値を空のままにします。その場合、同期はすべてのユーザーとグループがします。
   (LDAP の root オプションのような)
2. グループ/グループ名 -同期を開始したいグループを入力し、特定のグループから同期します。Azureグループはすべて同じレベルで開かれており、他のどのグループがどのグループに接続されているかを示すポインタを持っています。
   その場合、深度を使用すると、設定された検索深度の値に従って、元の開始グループに接続されている他のグループがスキャンされます。開始ノード名をStart Sync Fromで変更します。

目的地と時刻の情報アイコン内の以下のテキストを更新します。
開始ノード: 同期をどこから開始するかを定義します。ディレクトリ内のすべてのユーザーとグループを同期するには空のままにするか、開始したいグループ"groups/**groupname**"を指定します。構成が完了した

ら、「テスト」をクリックしてドメインが有効であることを確認します (テストが完了するまでに最大 2 分かかる場合があります)。

インラインテキスト:すべてのディレクトリを同期するには空のままにするか、*groups/**<group name>***を入力します*(1グループのみ許可)*。



オブジェクト

オブジェクトの種類

バージョン 1 のオブジェクト タイプ「コンピュータ」はサポートされていません。代わりに、Azure AD にはdevicesがあります。しかし、まだ調査する必要があります。コンピューターのオプションを削除してください。
「オブジェクト」タブの情報テキストを更新します。オブジェクトの同期: どのオブジェクトを同期するかを構成します (現在、ユーザーオブジェクトのみがサポートされています)

同期属性

Azure ディレクトリのデフォルト値は UserPrincipalName です。CN と SAMaccountName を DD リストから削除してください。ユーザーは同期したい属性を入力できます (フリーテキスト)。

メンバーシップフィルター:

Azure ディレクトリが選択されている場合、DD リストが更新されて 2 つのオプションが表示されます

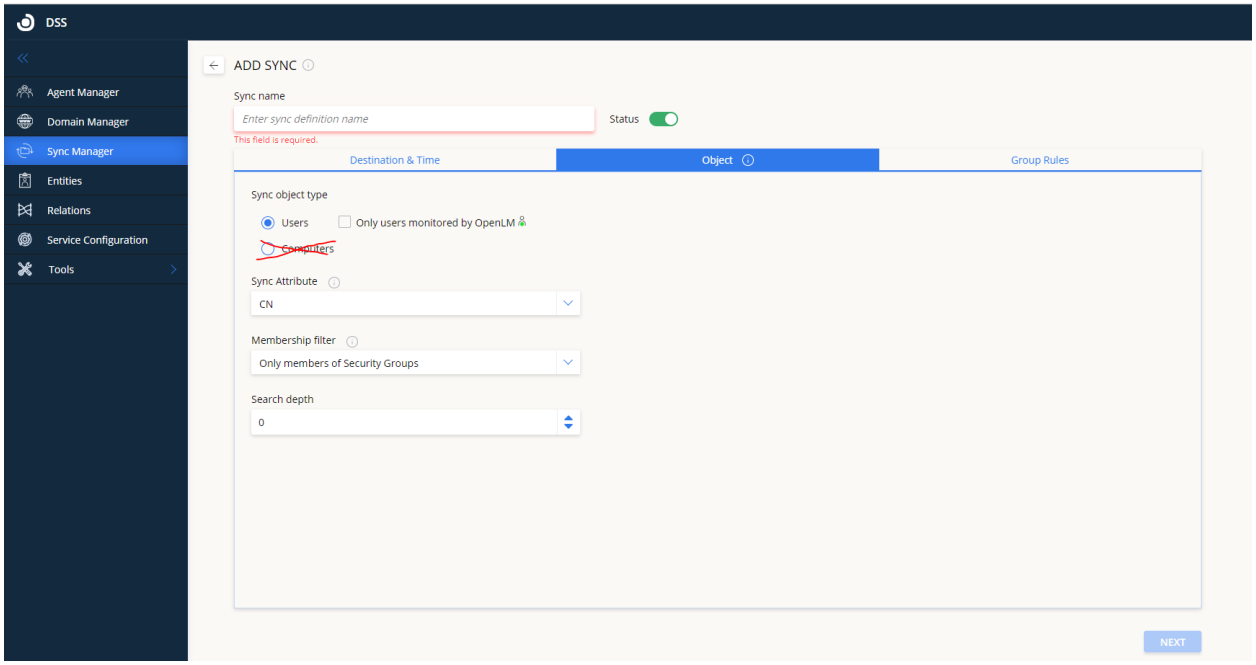
1. すべてのオブジェクト
2. グループメンバーのみ

Azure AD には OU がなく、代わりにAdministrative unitsがありますが、これらのユニットの下に他のユニットを保持することはできません。バージョン 1 についてはサポートされません。

メンバーシップ フィルターの情報アイコンを更新します (Azure Active Directory が選択されている場合のみ)メンバーシップフィルター
すべてのオブジェクトを同期するかどうかを選択します。またはグループに属するもののみ。

検索の深さ

検索の深さは、グループの「開始ノード」を操作する場合にのみ関係します。。
「Start Sync From」がグループを示している場合のみ、ユーザーが検索の深さを入力できるようにする。それが空の場合は、「同期開始元」グループを設定しない限り、検索の深さは 0 にする必要があります。」というエラー メッセージが表示されます。



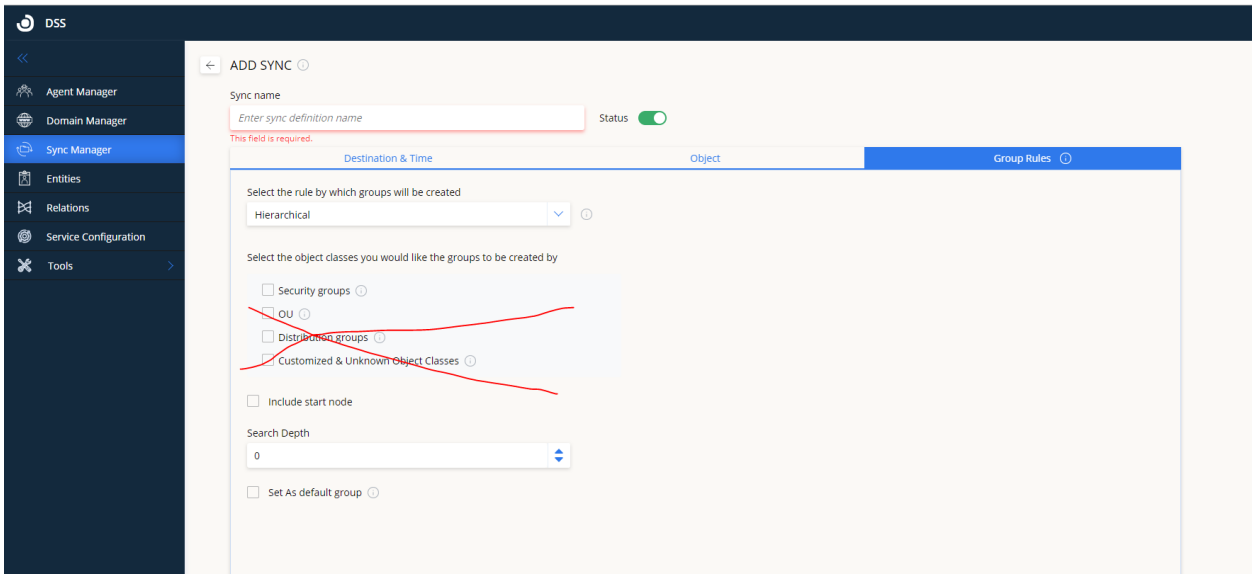
グループルール

すべてのグループ ルールがサポートされています (標準 LDAP と同じリスト)。hierarchy synchronizationはグループ のみをサポートします。したがって、チェックボックスを選択する必要はありません。
「グループの作成に使用するオブジェクトクラスを選択してください」の代わりに「階層グループは、以下で指定したグループと検索の深さに従って作成されます」と書きます。

残りのオプション (OU、ディストリビューショングループ、カスタマイズおよび不明なオブジェクトクラス) を削除してください。

開始ノードを含める: 開始グループを含めるに変更します。
検索の深さ -オブジェクト画面で選択した検索深度を超えることはできません。
デフォルトグループの設定 - サポートされています

「開始ノードを含める」を「開始グループを含める」に変更します (開始グループに接続しているユーザーを取得し、開始グループ名の下にグループとして追加します)。



ディレクトリサンプル
ディレクトリにはグループ A ～ E があります
→ あるグループから別のグループへのポインタを示します

A → B
B→C

C→D
C→A
D→E
E

ユーザーリスト:
グループ A - U5、U6
グループ B - U7、U8
グループ C - U1、U2、U3、U4
グループ D - U9、U10
グループ E - U11、U12

グループとルールの検索深さ 3 で Groups\C から同期するように同期が構成されている場合の階層構造

C--
    A--
        B--
    D--
        E

U1
U2
U3
U4
    U5
    U6
        U7
        U8
    U9
    U10
        U11
        U12