ORACLE

Oracle Client 23ai のLDAP URL構文

簡単なアプリケーション構成用のLDAP構文

2024年8月、バージョン1.0

ORACLE

本書の目的

本書では、Oracle Database 23aiの機能および強化点の概要を説明しています。本書は、アップグレードに関するビジネス上の利点の評価と、説明した製品機能の実装およびアップグレードの計画を支援することのみを目的としています。

免責事項

本文書には、ソフトウェアや印刷物など、いかなる形式のものも含め、オラクルの独占的な所有物である占有情報が含まれます。この機密文書へのアクセスと使用は、締結および遵守に同意したOracle Software License and Service Agreementの諸条件に従うものとします。本文書と本文書に含まれる情報は、オラクルの事前の書面による同意なしに、公開、複製、再作成、またはオラクルの外部に配布することはできません。本書は、ユーザーとのライセンス同意書の一部をなすものではなく、またオラクルやその子会社および関連会社とのいかなる契約上の合意事項にも含まれるものではありません。

本書は情報提供のみを目的としたものであり、ここで説明する製品の機能を実装およびアップグレードする際の資料として使用されることのみを意図しています。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料になさらないでください。本文書に記載されている機能の開発、リリース、時期および価格については、弊社の裁量により決定されます。製品アーキテクチャの性質上、本書に記述されているすべての機能を安全に組み込むことができず、コードの不安定化という深刻なリスクを伴う場合があります。

ORACLE

目次

ORACLE

はじめに

Oracle Client 23aiの接続文字列の構文が改善されたため、Oracle Databaseへの接続時にディレクトリの名前解決用のLDAPが使いやすくなりました。この新機能により、Oracle DatabaseのEasy Connect構文が拡張され、LDAPおよびLDAPS接続がサポートされるようになりました。これにより、外部のLDAP構成ファイルが必要なくなるため、開発者がLDAPを使用しやすくなります。

ディレクトリ・ネーミングの概要

アプリケーションは、Oracle Databaseに接続するために、データベースのホストやサービス名などの情報を含む接続記述子を使用します。接続記述子は、さまざまな方法で指定できます。たとえば、アプリケーション・コードは、ローカルの*tnsnames.ora*構成ファイルに格納されている接続記述子にマッピングされている接続識別子を渡すことができます。代わりに、接続記述子を外部のマッピング・サービスに格納することもできます。使用可能な外部サービスの1つがディレクトリ・ネーミングです。これを使用すると、Oracle Internet Directory（OID）、Oracle Unified Directory（OUD）、Microsoft Active DirectoryなどのLDAP準拠のディレクトリ・サーバーに含まれる接続記述子にアプリケーションの接続識別子をマッピングできます。

ディレクトリ・ネーミングによって、ネットワークの名前とアドレスが1つの場所で一元化され、名前の変更と更新が簡単に管理できるようになります。これにより、クライアント・マシンの大規模ネットワークに格納されている*tnsnames.ora*ファイルに対する接続記述子の更新を管理者が管理する負担が解消されます。

LDAP URLの概要

Oracle DatabaseのLDAP名前参照は従来、ディレクトリ・サーバー名、ポート、接続コンテキストが含まれる外部の*ldap.ora*ファイルおよび*sqlnet.ora*ファイルの助けを借りてアプリケーション・ホスト上で構成されます。

Oracle Client 23aiには、URLをアプリケーションの接続文字列として使用する、LDAP参照の別の方法が導入されています。このURLには、以前は*ldap.ora*ファイルおよび*sqlnet.ora*ファイルに格納する必要があった値を含めることができます。LDAP URL構文を使用すると、Oracle Client 23aiのライブラリを使用しているアプリケーションから任意のデータベース・バージョンに接続できます。

LDAP URL構文

Oracle Client 23aiのLDAP URL構文は、次のとおりです。

protocol://host[:port]/alias[,context][?parameter1=value1{&parameter2=value2...}]

例：

ldaps://mydirserver.example.com/sales

次の表では、オプションについて説明します。プロトコル、ホスト名、エイリアスは必須です。

オプション	説明
protocol	プロトコルは、ldapまたはldapsになります。ldaps プロトコルはTLSを使用します。
host	LDAPディレクトリ・サーバーが動作しているホスト名。
port	LDAP接続用のオプションのポート番号。 LDAPプロトコルのデフォルトのポートは389であり、LDAPSプロトコルのデフォルトのポートは636です。
alias	データベースの接続記述子の取得元のLDAPエントリ。このエントリは、指定のコンテキストの OracleContextコンテナに含まれている必要があります。
context	オプションのディレクトリ・ネーミング・コンテキストで、 OracleContextが含まれます。たとえば、コンテキストは cn=OracleContext,dc=example,dc=comのようになります。

	このデフォルト値はcn=OracleContextです。
parameters	オプションのパラメータは、LDAP接続を定義する名前/値ペアです。 パラメータについては、次の表で説明します。

オプションのURLのパラメータ

LDAP URL構文は、接続の動作を定義する、大文字と小文字を区別しない、オプションのパラメータを4つサポートしています。デリミタ“?”は、パラメータの開始を示します。個々のパラメータはデリミタ“&”によって区切られます。パラメータは位置とは無関係です。パラメータ間の空白は無視されます。

注意すべき点として、TLSまたはmTLSデータベース接続にウォレットが必要である場合、ウォレットの場所は、LDAP URLのWALLET_LOCATIONパラメータ内ではなく、*sqlnet.ora*ファイル内、またはLDAPサーバー・エントリに格納されている接続記述子のWALLET_LOCATIONパラメータ内に指定する必要があります。

パラメータ名	説明
DIRECTORY_SERVER_TYPE	LDAPベースの名前参照に使用されるディレクトリ。値は、*OID*または*AD*になります。 OUDを使用している場合、OUDとOIDのネーミングは同じであるため、この値はデフォルトのままにします。 デフォルトは*OID*です。
AUTHENTICATE_BIND	LDAPネーミング・アダプタが、LDAPディレクトリへの接続時に、指定されたウォレットを使用して認証を試みる必要があるかどうかを指定します。 *TRUE*である場合、LDAP接続は、場所をWALLET_LOCATIONパラメータに指定する必要があるウォレットを使用して認証されます。 *FALSE*である場合、LDAP接続は、匿名のバインドを使用して確立されます。 デフォルト値は*FALSE*です。
AUTHENTICATE_BIND_METHOD	クライアントのLDAPネーミング・アダプタがLDAPディレクトリに接続して接続識別子を解決するときに使用する必要がある認証方式を指定します。 ディレクトリ・エントリのDNとパスワードはOracle Wallet内に格納できます。クライアントがLDAPサーバーに接続する場合、このウォレット内に格納されている資格証明を使用して認証されます。ウォレットの信頼ストアには、LDAPサーバーの認証局によって発行されたルート証明書が含まれている必要があります。 LDAPネーミング・アダプタは、LDAPサーバーでの認証のためにウォレットのoracle.ldap.client.dnエントリおよびoracle.ldap.client.passwordエントリを使用します。これらのエントリが存在しない場合、クライアントは、TLSまたはLDAPSを使用して匿名認証を試みます。 たとえば、次のとおりです。 AUTHENTICATE_BIND_METHOD=ldaps_simple_auth
WALLET_LOCATION	ウォレットが格納されているディレクトリを指定します。このウォレットは、LDAPサーバーに対するTLS接続を確立するために使用されます。このパラメータは、データベース接続には適用できません。URLにWALLET_LOCATIONが指定されていない場合、*sqlnet.ora*でウォレットの場所が確認されます。WALLET_LOCATIONが*sqlnet.ora*に設定されていない場合、オペレーティング・システムの証明書ストアが使用されます。

ユースケース

このセクションでは、Oracle Client 23aiのLDAP URL構文の例を示します。この例では、ディレクトリ・エントリcn=orcl,cn=OracleContext,dc=example,dc=comを検索します。

例1

基本的な使用方法の例。URL文字列にユーザー・ウォレットが指定されていない場合、クライアント・ライブラリは、sqlnet.oraファイルでユーザー・ウォレットを確認します。ユーザー・ウォレットが見つからない場合、デフォルトのオペレーティング・システムのデフォルトの証明書ストアが使用されます。

ldaps://ldapserver.example.com/cn=orcl,cn=OracleContext,dc=example,dc=com

Oracleのpython-oracledbドライバを使用する場合、これが次のように接続文字列として使用される可能性があります。

```
cs = "ldaps://ldapserver.example.com/cn=orcl,cn=OracleContext,dc=example,dc=com"
connection = oracledb.connect(user="scott", password=pw, dsn=cs)
```

例2

OIDの簡易認証を使用した例。LDAPバインド操作の資格証明は、指定されたウォレットから取得されます。

ldaps://ldapserver.example.com/cn=orcl,cn=OracleContext,dc=example,dc=com?WALLET_LOCATION=/app/wallet&AUTHENTICATE_BIND=true&AUTHENTICATE_BIND_METHOD=LDAPS_SIMPLE_AUTH

相互TLS（mTLS）LDAP認証の場合：

ldaps://ldapserver.example.com/cn=orcl,cn=OracleContext,dc=example,dc=com?WALLET_LOCATION=/app/wallet&AUTHENTICATE_BIND=true

例3

Active Directoryの簡易認証を使用した例。LDAPバインド操作の資格証明は、指定されたウォレットから取得されます。

ldaps://ldapserver.example.com/cn=orcl,cn=OracleContext,dc=example,dc=com?DIRECTORY_SERVER_TYPE=AD&WALLET_LOCATION=/app/wallet&AUTHENTICATE_BIND=true&AUTHENTICATE_BIND_METHOD=LDAPS_SIMPLE_AUTH

Windowsのネイティブ認証を使用したActive Directory（Windowsのログイン資格証明を使用）：

ldap://ldapserver.example.com/cn=orcl,cn=OracleContext,dc=example,dc=com?DIRECTORY_SERVER_TYPE=AD&AUTHENTICATE_BIND=true

例4

クリア・テキストのポートを使用したLDAPサーバーへの接続の例：

ldap://ldapserver.example.com/cn=orcl,cn=OracleContext,dc=example,dc=com

まとめ

Oracle Client 23aiのライブラリを使用したアプリケーションは、LDAPサーバーのディレクトリの名前解決用として、新しい、オプションの、簡単なURL構文を活用できます。これは、任意のOracle Databaseバージョンへの接続をサポートしています。この新しい構文により、LDAPが使いやすくなり、従来のLDAP構成ファイルをクライアント・マシンに分散させるオーバーヘッドが解消されます。

その他のお勧め情報として、接続情報とアプリケーション構成情報をAzure App ConfigurationストアまたはOracle Cloud Infrastructure（OCI）Object Storageに格納することを可能にする、新しいOracle Databaseの一元化された構成プロバイダ機能をご確認ください。

ORACLE

参考資料

ドキュメント：「接続識別子でのLDAPパラメータの直接指定」

技術概要：OIDおよびOUDのディレクトリ・ネーミングのためのOracle Databaseクライアントの構成

技術概要：Microsoft Active Directoryネーミングのためのクライアントの構成

ORACLE

Connect with us

+1.800.ORACLE1までご連絡いただくか、**oracle.com**をご覧ください。北米以外の地域では、**oracle.com/contact**で最寄りの営業所をご確認いただけます。

blogs.oracle.com facebook.com/oracle twitter.com/oracle