Oracle Netネーミングを実行するための Microsoft Active Directoryの構成

Oracleホワイト・ペーパー
2014年4月

Oracle Netネーミングを実行するためのMicrosoft Active Directoryの構成

はじめに

Oracle Netネーミング・メソッドにより、名前がデータベースの接続記述子に解決されます。ネーミング・メソッドの1つには、ディレクトリ・ネーミング・メソッドが挙げられます。ディレクトリ・ネーミングでは、Oracle Internet DirectoryやMicrosoft Active Directoryなどの一元化されたLDAP準拠のディレクトリ・サーバーに格納されたデータベース・サービス名、ネット・サービス名、またはネット・サービスのエイリアスが解決されます。データベース・サービスおよびネット・サービス名の集中管理により、追加または再配置が容易になります。ユーザーが接続文字列を指定すると、接続リクエストが開始されます。接続文字列には、ユーザー名とパスワードに加えて、接続識別子が含まれます。接続識別子は、接続記述子自体にすることも、接続記述子に解決される名前にすることもできます。

ディレクトリ・ネーミングで提供される機能をオラクル製品で使用するために、Active Directoryを構成する必要があります。これには、Active Directorスキーマ・オブジェクトの拡張と、OracleContextコンテナの作成が含まれます。Oracleスキーマ・オブジェクトとは、Active Directoryに格納されるOracle Net ServicesおよびOracle Databaseのエントリとその属性に関する一連のルールです。Active Directoryの名前解決では、データベース・サービスおよびネット・サービス名の集中管理が提供され、企業の既存のWindows環境が活用されることで、サービスの追加または再配置が容易になります。

Active Directoryを使用したOracle Netネーミングは、Windowsホストのクライアントでサポートされています。サービス（データベース）はすべてのマシンで実行されます。必ずしもWindowsホストにする必要はありません。

このホワイト・ペーパーでは、Oracle Database 11g Release 2（11.2.0.3）以降に対して、Windows Server 2008以降でのネット・サービスのネーミングをサポートするために、Active Directoryを構成する詳細な手順について説明します。

Oracle Netネーミングに対応するようにActive Directoryを構成するおもな手順は、次のとおりです。

- Active Directory の匿名参照の有効化
- NetCA による Oracle コンテキストの作成
- 表示指定子の作成

Active Directoryの構成手順

Active Directoryドメイン・コントローラになるようにWindows Serverを昇格させたら、Oracleコンテキストを作成できるようにActive Directoryを構成する必要があります。

匿名参照の有効化

Windows Server Active Directoryでは、認証されたユーザーのみが、Windows Serverベースのドメイン・コントローラに対してLDAPリクエストを開始できます。匿名参照の有効化には、LDAPブラウザまたは修飾子が必要です。必要な属性値を変更するもっとも簡単な方法は、Windows ADSI Editユーティリティを使用することです。

ADSI Editを起動するには、Windowsコマンド・ウィンドウからadsiedit.mscコマンドを発行します。または、MMCコンソール・ルートで、「ファイル」→「スナップインの追加と削除」→「追加」をクリックして、「ADSI Edit」を選択し、「追加」→「閉じる」→「OK」をクリックします。「ADSI Edit」を選択して右クリックして、「Connect to」をクリックし、「Configuration Naming Context」を選択して、「OK」をクリックします。

Configurationコンテナを展開し、次の場所に移動します。

Configuration [acme.com]

CN=Configuration, DC=ACME, DC=COM CN=Services

CN=Windows NT

CN=Directory Service

CN=Directory Serviceコンテナを右クリックして、「プロパティ」を選択し、下にスクロールして「dSHeuristics」属性を選択します。

dSHeuristics属性を編集して、その値を0000002に設定します。この値に設定すると、匿名のクライアントで、アクセス制御リスト（ACL）で許可されたすべての操作を実行できるようになります。

スキーマの拡張およびOracleコンテキストの作成

Active DirectoryとともにOracle Netディレクトリ・ネーミング機能を使用するには、Oracleコンテキストを作成する必要があります。Oracleコンテキストは、Active Directoryツリーの最上位のOracleエントリです。これには、Oracle DatabaseサービスおよびOracleネット・サービス名のオブジェクト情報が含まれます。

Oracle Netネーミングを実行するためのMicrosoft Active Directoryの構成

Oracle Net Configuration Assistant（Oracle NetCA）を使用して、スキーマを拡張し、Oracleコンテキストを作成します。Oracle NetCAはグラフィカルな、ウィザードベースのツールです。これを使用してオラクル製品のネットワークを構成し、その構成を管理できます。Oracleコンテキストは、Oracle Databaseのカスタム・インストール中、またはカスタム・インストール後に作成できます。

作成できるOracleコンテキストは、Windowsドメイン（管理コンテキスト）ごとに1つだけです。Oracle Net Configuration Assistantを使用して、Active DirectoryにOracleコンテキストを作成するには、ドメインおよびエンタープライズ・オブジェクトを作成する権限が必要です。

1. Network Configuration Assistantを実行します。
   a) 「スタート」をクリックしてから、「すべてのプログラム」をクリックします。
   b) 「Oracle」→「Configuration and Migration Tools」→「Net Configuration Assistant」をクリックします。
2. 「Directory Usage Configuration」ラジオ・ボタンを選択し、「next」をクリックします。
3. 「Directory Type Microsoft Active Directory」を選択し、「next」をクリックします。

   注：Microsoft Active Directoryの構成オプションは、Oracle NetCAのWindowsバージョンでのみ使用できます。
4. オラクル製品で使用するディレクトリを構成してOracleスキーマおよびコンテキストを作成するオプションを選択し、「next」をクリックします。
5. Active Directoryのホスト名を入力し、「next」をクリックします。初めてフォレストを構成する場合は、スキーマ・マスター・コントローラのホスト名を入力し、スキーマ・オブジェクトの作成権限を持つそのドメインのユーザーとしてログインする必要があります。
6. Oracleスキーマをアップグレードするオプションを選択し、「next」をクリックします。
7. 次のページに、ディレクトリ構成に成功したことが示されます。

   Directory usage configuration complete!
   Example:The distinguished name of your default Oracle Context is:
   Cn =OracleContext, DC=ACME, DC=COM
8. 「next」をクリックして、「Finish」をクリックします。

Active Directory を使用して Oracle スキーマ・オブジェクトを作成する場合、次の制限事項が適用されます。

フォレストごとに作成できるOracleスキーマ・オブジェクトは1つだけです。

ルート・ドメイン・コントローラをスキーマの更新を許可する操作マスターにする必要があります。手順についてはオペレーティング・システムのドキュメントを参照してください。

24のデフォルト言語すべてが許可されるようにActive Directoryの表示が構成されていない場合は、Oracle Net Configuration AssistantがActive Directoryをディレクトリ・サーバーとして構成しているときに、Oracleスキーマ・オブジェクトの作成が失敗する可能性があります。Oracle Net Configuration Assistantを実行してディレクトリ・アクセスの構成を完了させる前に、コマンド・プロンプトに次のコマンドを入力して、24言語すべての表示指定子が設定されていることを確認します。

```
ldifde -p OneLevel -d cn=DisplaySpecifiers,
cn=Configuration, domain context -f temp file
```

コマンドの意味は次のとおりです。

*domain context*は、このActive Directoryサーバーのドメイン・コンテキストです。たとえば、`dc=example, dc=com`です。

*temp file*は、出力先とするファイルです。

コマンドのレポートで検出されたエントリが24個未満の場合でも、引き続きOracle Net Configuration Assistantを使用できます。ただし、このレポートでは、Oracleスキーマ・オブジェクトの作成が失敗したことが示されています。単純に一部の言語の表示指定子が作成されなかったことを報告しているわけではありません。

表示指定子の作成

Net Configuration AssistantによってActive DirectoryにOracleスキーマ・オブジェクトが作成される場合、Oracleエントリの表示指定子は作成されません。これは、Active Directoryインタフェースに Oracleデータベースのエントリを表示できないことを意味しています。

Oracleスキーマ・オブジェクトの作成後に、Net Configuration AssistantでOracleスキーマ・オブジェクトを作成したときに使用したものと同じWindowsユーザーIDを使用して次の手順を実行することで、これらのエントリをActive Directoryに手動で追加できます。

1. コマンド・シェルを開きます。
2. ディレクトリをORACLE_HOME\ldap\schema\adに変更します。
3. adDisplaySpecifiers_us.sbsをadDisplaySpecifiers_us.ldifにコピーします。
4. adDisplaySpecifiers_other.sbs を adDisplaySpecifiers_other.ldif にコピーします。

5. これらの.ldifファイルをそれぞれ編集します。すべての%s_AdDomainDN%を、表示指定子のロード先となる特定のActive DirectoryのドメインDN（dc=acme, dc=comなど）で置き換えます。
6. 次のコマンドを実行します。

ldapmodify -h <ad hostname> -Z -f adDisplaySpecifiers_us.ldif

ldapmodify -h <ad hostname> -Z -f adDisplaySpecifiers_other.ldif

ここで<ad hostname>は、表示指定子のロード先となるActive Directoryドメイン・コントローラのホスト名です。

OracleContextが正常に作成されると、Active DirectoryでNetServicesとDatabaseServicesを格納できるようになります。Oracle Net ManagerまたはOracle Enterprise Managerを使用して、Active Directoryでサービス名を作成できます。

ネット・サービス名に対するデフォルトのアクセス制御リスト（ACL）では、それらの属性の匿名読取りは許可されません。Oracleクライアントで名前解決のために匿名バインドが有効化されている場合は、匿名読取りを許可するようにOracleContextおよびネット・サービス名に対するACLを変更する必要があります。Oracle Database 11g以降では、データベース管理者が、サービスに対するACLで利用可能なサービスが認証および制御されるようにOracleクライアントを構成して、サービスへのアクセスを制限できます。Active Directoryへの接続時にLDAPネーミング・アダプタで認証が試行されて、接続文字列の名前が解決されるかどうかを指定する場合は、sqlnet.oraでNAMES.LDAP_AUTHENTICATE_BIND=TRUEパラメータを使用します。Windowsクライアントでは、Active Directoryに対する認証に、ネイティブ認証方式が使用されます。

結論

Windows Server Active Directoryでは、認証されたユーザーのみが、Windows Serverベースのドメイン・コントローラに対してLDAPリクエストを開始できます。レジストリ・エントリを更新すると、Active Directoryの属性の1つがOracle NetCAディレクトリの正常な構成に役立ちます。これにより、Oracle Netネーミングが可能になります。

Oracle Netネーミングを実行するためのMicrosoft Active Directoryの構成
2014年4月
著者：**Srinivas Pamu**
共著者：**Kant Patel**
共著者：**Norman Woo**

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065 U.S.A.

海外からのお問い合わせ窓口：
電話：**+1.650.506.7000**
ファクシミリ：**+1.650.506.7200**

oracle.com