

Oracle® Enterprise Repository

LDAP/Active Directory インストール ガイド

10g リリース 3 (10.3)

2008 年 10 月

Oracle Enterprise Repository LDAP/Active Directory Installation Guide, 10g Release 3 (10.3)

Copyright © 2007, 2008, Oracle. All rights reserved.

原著者 : Vimika Dinesh

原協作者 : Scott Spieker, Jeff Schieli, Sharon Fay

このプログラム(ソフトウェアおよびドキュメントを含む)には、オラクル社およびその関連会社に所有権のある情報が含まれています。このプログラムの使用または開示は、オラクル社およびその関連会社との契約に記された制約条件に従うものとします。著作権、特許権およびその他の知的財産権と工業所有権に関する法律により保護されています。独立して作成された他のソフトウェアとの互換性を得るために必要な場合、もしくは法律によって規定される場合を除き、このプログラムのリバース・エンジニアリング、逆アセンブル、逆コンパイル等は禁止されています。

このドキュメントの情報は、予告なしに変更される場合があります。オラクル社およびその関連会社は、このドキュメントに誤りがないことの保証は致し兼ねます。これらのプログラムのライセンス契約で許諾されている場合を除き、プログラムを形式、手段(電子的または機械的)、目的に関係なく、複製または転用することはできません。

このプログラムが米国政府機関、もしくは米国政府機関に代わってこのプログラムをライセンスまたは使用する者に提供される場合は、次の注意が適用されます。

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

このプログラムは、核、航空産業、大量輸送、医療あるいはその他の危険が伴うアプリケーションへの用途を目的としておりません。このプログラムをかかる目的で使用する場合、上述のアプリケーションを安全に使用するために、適切な安全装置、バックアップ、冗長性(redundancy)、その他の対策を講じることは使用者の責任となります。万一かかるプログラムの使用に起因して損害が発生いたしましても、オラクル社およびその関連会社は一切責任を負いかねます。

Oracle, JD Edwards, PeopleSoft, Siebelは米国Oracle Corporation およびその子会社、関連会社の登録商標です。その他の名称は、他社の商標の可能性があり得ます。

このプログラムは、第三者のWebサイトへのリンク、第三者のコンテンツ、製品、サービスへアクセスすることがあります。オラクル社およびその関連会社は第三者のWebサイトで提供されるコンテンツについては、一切の責任を負いかねます。当該コンテンツの利用は、お客様の責任となります。第三者の製品またはサービスを購入する場合は、第三者と直接の取引となります。オラクル社およびその関連会社は、第三者の製品およびサービスの品質、契約の履行(製品またはサービスの提供、保証義務を含む)に関しては責任を負いかねます。また、第三者との取引により損失や損害が発生いたしましても、オラクル社およびその関連会社は一切の責任を負いかねます。

Oracle Enterprise Repository

LDAP/Active Directory インストール ガイド

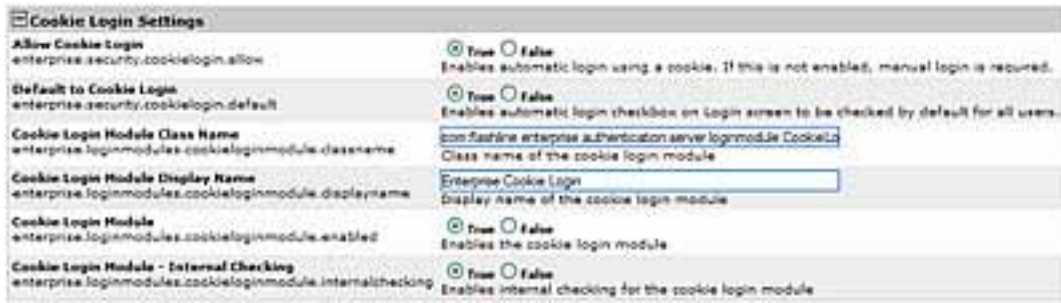
LDAP / Active Directory を利用してユーザを認証する場合、LDAP/Active Directory サーバを使用する前に、ユーザの部門およびロールのコンフィグレーションを検討する必要があります。統合が有効になると、以降はすべてのユーザが LDAP/AD 経由で認証されます。LDAP/AD のユーザ名と一致する管理レベルのユーザ アカウントが Oracle Enterprise Repository データベース内に 1 つ以上作成されていることが不可欠です。LDAP/AD が有効なときに Oracle Enterprise Repository 内の管理機能を引き続き実行できるように、このユーザ アカウントは admin ロールに割り当てする必要があります。

LDAP/AD からのロールの同期が有効な場合は、1 つ以上のユーザ アカウントが管理レベルのロールに割り当てられている必要があります。ロール同期オプションを使用する前に、LDAP ロールが作成され、Oracle Enterprise Repository 内で適切な OER パーミッションが割り当てられている必要があります。ロール名は名前のみが同期されます。管理レベルのユーザが LDAP/AD を利用して Oracle Enterprise Repository にログインした場合は、そのユーザはアプリケーションを適切にコンフィグレーションおよび管理することができます。このユーザ アカウントは、日常のアクティビティに**使用しないでください**。

LDAP 統合システム プロパティの有効化

この手順は Oracle Enterprise Repository の [Admin] 画面で行われます。

1. 左ペインの [System Settings] をクリックします。
主ペインに [System Settings] セクションが開きます。
2. [Cookie Login Settings] グループで [Enterprise Authentication] セクションを探します。



3. [Allow Cookie Login] 設定が [False] に設定されていることを確認します。
4. [System Settings Search] ボックスを使用して、以下の各設定を簡単に検索します。
5. 検索ボックスに「enterprise.authentication.ldap.enabled」と入力します。値を [True] に設定して [Save] をクリックします。

以下に示すように、設定を変更します。それぞれの [True] または [False] の設定に特に注意してください。

- [Default to Cookie Login]
 - [False] に設定します。
- [Unapproved User Login]
 - [True] に設定します。
- [Cookie Login Module]
 - [False] に設定します。
- [Cookie Login Module - Internal Checking]
 - [False] に設定します。
- [Plug-in Login Module Class Name]
 - テキストボックスに「com.flashline.enterprise.authentication.server.loginmodule.LDAPLogin」と入力します。
 - **注意**：このプロパティは LDAP のオン/オフを切り替えます。有効にすると、アプリケーションはユーザ認証に LDAP サーバを使用します。
- [Plug-in Login Module Display Name]
 - テキストボックスに「Enterprise LDAP Login」と入力します。
- [Plug-in Login Module]
 - [True] に設定します。

- [Plug-in Login Module - Internal Checking]
 - [False] に設定します。

6. [Save] をクリックして終了します。

LDAP/Active Directory プロパティの変更

1. 左ペインの [System Settings] をクリックします。
2. [System Settings Search] を使用して、以下の各設定を簡単に検索します。以下に示すように、値を入力します。

それぞれの [True] または [False] の設定に特に注意してください。

- [LDAP Server Host Name]
 - テキスト ボックスに、ホスト名またはディレクトリ サーバの IP アドレスを入力します。
- [LDAP Server Port Number]
 - テキスト ボックスに「389」と入力します。
- [LDAP Mask]
 - LDAP の場合、「uid $\%=\wedge$ 」と入力します。
または...
 - Active Directory の場合、
「samAccountName $\%=\wedge$ 」と入力します。
- [Creation of Unapproved User Accounts]
 - [True] に設定します。
- [Assign default roles to users]
 - [True] に設定します。
 - **注意**：このプロパティは、ユーザ認証ごとにデフォルト ロールを割り当てます。
- [Auto create missing roles]
 - [True] に設定します。
 - **注意**：このプロパティは、LDAP/AD サーバから同期したロールを作成しますが、それらのロールに対してパーミッションは**割り当てません**。

- [Auto create missing departments]
 - [True] に設定します。
 - **注意** : このプロパティは、LDAP/AD サーバから同期した部門を作成しますが、それらの部門に対して説明は割り当てません。ただし、ユーザは新しいロールに割り当てられます。
- [LDAP Version]
 - テキスト ボックスに「3」と入力します(サポートされるバージョンは 2 および 3 です)。
- [Administrator Account Distinguished Name]
 - **注意** : このプロパティは、Active Directory の使用時に必要になります。このプロパティには、少なくとも読み取り専用のディレクトリ検索パーミッションを持つユーザ アカウントの DN を含める必要があります。
 - 例 : **CN=Some_User,CN=Users,DC=ad,DC=example,DC=com**
- [Administrator Account Password]
 - テキスト ボックスに、上記の [Administrator Account Distinguished Name] プロパティに指定した管理者アカウントのパスワードを入力します。
- [Use SSL Connection]
 - [True] に設定して、LDAP の SSL 接続を有効にします。デフォルトは [false] です。
- [Follow referrals]
 - [True] に設定します。
- [Retrieve data using the admin account]
 - LDAP では (該当する場合)、[False] に設定します。
 - Active Directory 環境または制限された LDAP 環境では、[True] に設定します。
- [Search Start Location]
 - **注意** : このプロパティは、ディレクトリ ツリーのどこからユーザ レコードの検索を開始するかを定義します。
 - 例 :
 - LDAP の場合 :OU=MemberGroupB, O=en_us
 - Active Directory の場合 :CN=Users,DC=ad,DC=example,DC=com
- [Search Scope]

- ドロップダウンから [subtree] を選択します。
 - **注意** : このプロパティは、ユーザ レコード検索の深さ (baseDN より下) を定義します。
- [Attribute Name that Identifies a Found Entry]
 - **注意** : このプロパティは、ツリー検索のスコープ内にあるユーザ アカウントを一意に識別する属性名を指定します。
 - LDAP の場合: `uid`
 - Active Directory の場合 : `samAccountName`
- [Found Entry Email Attribute Name]
 - 「`mail`」と入力します。
- [Found Entry First Name Attribute Name]
 - 「`givenName`」と入力します。
- [Found Entry Middle Name Attribute Name]
 - LDAP または Active Directory (該当する場合) のミドル名の属性を入力します。
- [Found Entry Last Name Attribute Name]
 - 「`sn`」と入力します。
- [Found Entry Telephone Number Attribute Name]
 - 「`telephoneNumber`」と入力します。
- [Use LDAP Departments]
 - [True] に設定します。
 - **注意** : このプロパティは、Oracle Enterprise Repository 内で同期されるユーザの部門属性の値を定義します。
- [Department Attribute]
 - 「`department`」と入力します。
- [Use LDAP Roles]
 - [False] に設定します。
- [Role Attribute]
 - ユーザのロール情報を含む LDAP / Active directory 属性を入力します。

○ [Second Level Lookup Attribute]

- **注意**：このプロパティは、ユーザ情報を取得するための第 2 レベルのルックアップを識別する属性を定義します。値は DN にする必要があります。第 2 レベルのルックアップにリダイレクトを使用している場合、この第 2 ルックアップには基本の DN を定義してください。

3. [Save] をクリックして終了します。

4. Oracle Enterprise Repository アプリケーションを再起動します。

セキュリティに関する考慮事項

Oracle Enterprise Repository LDAP/Active Directory Connector を使用すると、LDAP が Oracle Enterprise Repository のユーザ認証およびロール割り当てにおけるユーザ識別の単一ソースとして機能します。ただし、これによって、各ホスト リポジトリで Oracle Enterprise Repository 経由でのファイル アクセスのユーザ認証を管理する必要がなくなるわけではありません。

Oracle Enterprise Repository LDAP/Active Directory Connector を使用した場合、Oracle Enterprise Repository は LDAP または Active Directory を利用してユーザを認証します。ユーザ名とパスワードの組み合わせは、バインド要求として LDAP システムに委任されます。バインド要求が成功した場合にのみ、ユーザが認証されます。

オプションとして、Oracle Enterprise Repository のユーザ ロール割り当てを格納および取得するように、LDAP をコンフィグレーションできます。このコンフィグレーションでは、ロールが LDAP に格納されるように、ユーザ ログインのたびに Oracle Enterprise Repository がユーザのロールと同期します。ロールは LDAP 経由で直接追加され、Oracle Enterprise Repository では管理されません。

使用例のサンプル シナリオ

以下のシナリオでは、LDAP セットアップおよびコンフィグレーションの選択を示して、ユーザ管理のプロパティ設定を明示します。

シナリオ 1

LDAP 認証の場合に、Oracle Enterprise Repository へのユーザ アクセスを防止します。アクティブな Oracle Enterprise Repository アカウントを持つ既存のユーザに対してのみ、アクセス権を提供します。

- **原理**
 - ユーザベースが事前定義されており、アプリケーションに対して許可されるユーザ数が制限された非エンタープライズ使用許諾契約。
- **プロパティ設定**
 - `ldap.allow-user-creation`
 - [False] に設定します。
 - `enterprise.security.unapproveduser.allowlogin`
 - [False] に設定します。

シナリオ 2

LDAP 認証の場合に、デフォルトの Oracle Enterprise Repository ユーザ アカウントを作成してデフォルトのロールを割り当てますが、Oracle Enterprise Repository へのユーザ アクセスは拒否します。

- **原理**
 - セキュリティ管理者が新規ユーザ アカウントが作成されたという通知を受け取るまで、新規ユーザに対して Oracle Enterprise Repository アクセスを拒否するため。セキュリティ管理者によって承認されると、以降はユーザの状態がアクティブに変更され、Oracle Enterprise Repository のログインが許可されます。
- **プロパティ設定**
 - `ldap.allow-user-creation`
 - [True] に設定します。
 - `ldap.assign-default-roles`
 - [True] に設定します。
 - `enterprise.security.unapproveduser.allowlogin`
 - [False] に設定します。

シナリオ 3

LDAP 認証で、デフォルト ロールを使用してデフォルトの Oracle Enterprise Repository ユーザ アカウントが作成され、そのユーザは Oracle Enterprise Repository へのログインを許可されます。

- **原理**

- LDAP 認証が新規ユーザの作成に対する唯一の制限事項であるエンタープライズ使用許諾契約。通常は、LDAP アカウントによってロールが事前定義されていない新規ユーザのアクセス権を制限するために、デフォルトの Oracle Enterprise Repository ロールが [User] に設定されます。

- **プロパティ設定**

- `ldap.allow-user-creation`
 - [True] に設定します。
- `ldap.assign-default-roles`
 - [True] に設定します。
- `enterprise.security.unapproveduser.allowlogin`
 - [True] に設定します。

LDAP プロパティの例

ディレクトリ サーバに匿名でバインドされている (認証されていない) 間は、Active Directory の制限によって最上位より下のディレクトリが検索されないため、Oracle Enterprise Repository ユーザ情報のルックアップでは、[Bind DN]、[Bind Password]、および [Retrieve Data As Admin] プロパティを適切な値に設定する必要があります。

| Active Directory | | Traditional LDAP (InetOrgPerson) | |
|-----------------------------|--|----------------------------------|------------------------------|
| ldap.host | ad.example.com | ldap.host | ldap.example.com |
| ldap.port | 389 | ldap.port | 389 |
| ldap.version | 3 | ldap.version | 3 |
| ldap.bindDN | CN=Some_User, OU=Users,DC=ad, DC=example,DC=com | ldap.bindDN | (匿名でのルックアップが無効な場合は必須) |
| ldap.bindPassword | パスワード | ldap.bindPassword | (匿名でのルックアップが無効な場合は必須) |
| ldap.retrieve-data-as-admin | true | ldap.retrieve-data-as-admin | false (匿名ルックアップが無効な場合は TRUE) |
| ldap.mask | sAMAccountName=^ | ldap.mask | uid=^ |
| ldap.baseDN | CN=Users,DC=ad, DC=example,DC=com | ldap.baseDN | OU=MemberGroupB, O=en_us |

| | | | |
|----------------------|-----------------|----------------------|-----------------|
| ldap.scope | subtree | ldap.scope | one |
| ldap.uniqueIDAttrib | samAccountName | ldap.uniqueUDAttrib | uid |
| ldap.emailAttrib | mail | ldap.emailAttrib | mail |
| ldap.givennameAttrib | givenname | ldap.givennameAttrib | givenName |
| ldap.surnameAttrib | sn | ldap.surnameAttrib | sn |
| ldap.telephoneAttrib | telephonenumber | ldap.telephoneAttrib | telephoneNumber |
| ldap.deptAttrib | department | ldap.deptAttrib | department |

実装に関係ないカスタム プロパティおよび共通プロパティ

| | |
|--------------------------|---|
| ldap.rbac.mapperclass | com.flashline.enterprise.authentication.server.loginmodule.LDAPMapperImpl |
| ldap.deptAttrib | department |
| ldap.rbac.roleAttrib | roles |
| ldap.allow-user-creation | true |
| ldap.enable-synch-roles | true |
| ldap.enable-synch-depts | true |